‘INFORMATION AND TELECOMMUNICATIONS SECTOR VULNERABILITIES AND THREATS’

-

SEPTEMBER 2002

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
AT DARTMOUTH COLLEGE

IRIA/ISTS
45 Lyme Road
Hanover,
NH 03755
603-646-0700

Executive Summary

Section I – Information and Telecommunications Sector

The information and telecommunications (I&T) sector is crucial to the functioning of national and international political and economic systems. Virtually every other infrastructure sector's key assets are operated, monitored, or controlled by networked computers and other communication systems. This makes the I&T sector a highly attractive target for physical or cyber attacks that could seriously disrupt communications and the free flow of information, potentially resulting in cascading outages in other infrastructures.

Assets, Systems, Functions

The I&T sector consists of a vast array of assets, which include the following categories:

- Entry/exit points
- Cables
- Switches/routers
- Communication nodes
- Management and control systems

The I&T sector used to be comprised of two main meta systems: traditional circuit switched networks, mainly the wireline public telephone network, and packet-based Internet Protocol (IP) networks, primarily the Internet. A complex mix of systems and technologies is currently in use as communications move toward a unified, packet-based network architecture - what has been termed the Next Generation Network (NGN).[1]

The I&T sector's function is to deliver vast amounts of voice, electronic, and image data to government and business organizations and the general public quickly, efficiently and reliably, while maintaining the confidentiality, integrity and availability of that data.

Vulnerabilities

Vulnerabilities exist mainly in the form of critical communication nodes and systems. Critical communications nodes exist where different forms of communications data converge or key arteries for voice or Internet traffic come together.

Although a variety of different providers and systems (voice, data, wireless, microwave, satellite etc) exist in most markets, these systems often rely on, and interact with, one another. Different systems use the same resources to provide service or co-locate critical assets in the same physical location. In addition, phone and Internet networks frequently topologically mirror one another. This creates single points of failure – at least at the local and regional levels – that makes the sector vulnerable to attacks. Vulnerabilities may exist in the following areas:

- Shared Assets

[1] 'Convergence Task Force Report - Understanding Convergence and Interconnection of Emerging Networks – NGN Convergence: Security Issues and Recommendations', The President's National Security Telecommunications Advisory Committee, June 2001 - http://www.ncs.gov/nstac/ConvergenceReport-Final.htm

- Critical Nodes
  - Telco Hotels
  - NAPs
  - International Gateways
- Signaling and Control Systems
- Domain Name System

Fixed telephone networks are more centralized than Internet infrastructures and rely more heavily on a smaller number of assets.[2] The Internet is more dynamic and redundant, but data is more vulnerable – in transit and when stored on server and client machines. Online systems have repeatedly been found vulnerable to various forms of malware (worms, viruses, Trojans) and cyber attacks, such as denial of service (DoS) attacks and unauthorized intrusions (hacking).

Examples of I&T Infrastructure Damage:

- September 11, 2001
- Baltimore Train Accident

The most common cause of communications outages in the past has been physical damage to cables during construction work, other accidents, hardware or software flaws, or user errors. The I&T sector remains vulnerable to such occurrences.

Threats

Physical or cyber attacks could be launched against I&T infrastructure components in stand-alone attacks or in conjunction with other strikes. Hostile nation-states, perhaps in league with terrorist organizations, pose the most significant threat to the I&T infrastructure. Attacks could have a serious impact on national security and homeland defense. Possible economic and psychological effects should also be considered. Threats to the I&T infrastructure could take the following form:

- Physical Attacks
  - Electro-Magnetic Pulse / Radio Frequency Fields
- Cyber Attacks
  - Next-generation worms (multiple rapid propagation methods; damaging payloads; fusion of malware and hacking techniques).
  - Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks against DNS servers, routers or other key communication nodes.
  - Unauthorized intrusions (hacking) aimed at key communication nodes or systems, or crucial data servers.

Protective Measures

To best protect information and telecommunications systems, providers should adopt a strategy of defense in depth. This means that security should cover multiple layers, including application, network and perimeter security. If one layer is breached, additional

[2] See 'The Internet's Coming of Age', Computer Science and Telecommunications Board, 2001, P.81-84 - http://bob.nap.edu/html/coming_of_age/ and 'Trust in Cyberspace', Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, National Academy Press, Washington D.C., 1999, P.37/38 - http://www.nap.edu/books/0309065585/html/index.html

security measures are in place. A defense in depth strategy requires the use of firewalls, intrusion detection systems, anti-virus software, honeypots, and other security tools at various points on a system.
Other protective measures include:

- Physical, Geographic and Service Redundancy
- Physical Security
- Training and Awareness

New, more secure standards and protocols should be developed or applied where possible. This could include Internet Protocol version 6 (IPv6), Internet Protocol Security, the Emergency Telecommunications Service scheme, or IPSec for authenticated communications. Further, research and development (R&D) into new protocols and technologies could also help protect the sector. This R&D effort could be directed toward Free Space Optics, self-healing systems, biometrics technologies or better encryption schemes, among others.

Conclusions
Overall, the I&T sector is fairly resilient, robust and redundant. A variety of different communication methods and systems exist in parallel, and traffic can be re-routed around damaged system components in case of outage or attack. If service is disrupted, the distributed nature of the I&T sector means that it can quickly recover. This makes the likelihood of an attack that causes sustained international, national or even regional outages small.

However, a well-timed attack on specific communication nodes or assets could be used strategically to magnify the effects of other actions or to cause economic or psychological harm. Although the risk is low, a determined enemy with extensive planning capabilities and resources could target several or many critical communication nodes simultaneously in a coordinated strike. Such an attack could have serious consequences, such as total regional outages and national and international disruptions. The complexity of the I&T sector increases the risk of successful attacks, especially by insiders, as vulnerabilities or interconnections with other infrastructure sectors may be hidden.

Section II – Routers

Vulnerabilities
Routers are key Internet infrastructure components. They direct the flow of traffic around the web and their importance will be elevated as all communications traffic increasingly relies on IP-based data exchanges. Routers have been found vulnerable in a number of ways. They are often not as well secured, configured or monitored as other online systems. Further, they are prone to software vulnerabilities. The Border Gateway Protocol (BGP) is a potential avenue for hackers to attack a router or compromise it for attacks against other systems. Authentication of BGP messages between routers is currently inadequate. This leaves the potential for various forms of manipulation.

Possible Router Attacks
By exploiting router vulnerabilities a cyber attacker could:

- Take over or disrupt a router; disrupt neighboring routers

- Inject false routing information into the routing system
- Use routers as launch pads for scans or attacks against other systems

Attacks could result in data manipulation, Internet 'black holes', DoS attacks against certain nodes or networks, and slowdowns in the flow of data around the Internet.

Security

To defend routers against online threats the following measures should be implemented:

- Change default passwords
- Remove vendor back doors
- Properly configure devices
- Disable unnecessary services
- Apply sensible routing policies
- Increase system logging
- Conduct regular security audits

Other measures, like agreeing upon the introduction of a secure version of BGP (S-BGP) or providing routers with global information on the Internet's topology, could be more difficult to achieve.

Conclusions

Overall, the routing infrastructure is relatively robust, dynamic and redundant. Major backbone and ISP border routers are programmed to filter information so that the possibility of manipulation is decreased. In addition, static configurations of primary and backup routes are used by top-level ISPs.

Certain routers at the gateways between highly connected networks are vulnerable to attacks due to their strategic position. Further, a router's ability to respond effectively to an outage or attack may be limited. If an attack did occur, there may not be sufficient capacity elsewhere in the network to carry the traffic. This does not pose an immediate threat to the I&T infrastructure sector as a whole, although it does hold the scepter of isolated outages. As attack techniques develop and new vulnerabilities are discovered, a coordinated, large-scale attack on the Internet's routers becomes a more serious threat.

Table of Contents

Section I – Information and Telecommunications Sector

Introduction

Based on the new direction of national infrastructure protection efforts outlined in the President's 'National Strategy for Homeland Security', this report focuses on the Information and Telecommunications (I&T)[3] infrastructure sector. It provides a general sector overview, including listing assets, systems and functions, vulnerabilities and threats, and possible protective measures. The report also examines the role of routers in the I&T sector, and router security.

Critical government systems, military operations, economic and financial transactions, and society as a whole, are becoming ever more interactive and interconnected. Hence, reliance on, and the importance of, information and telecommunications infrastructures have grown. Dedicated networks exist in some areas for security reasons, but most systems vital to national security and economic prosperity are connected (directly or indirectly) to the public networks that make up the I&T sector.

Therefore, it is essential to gain understanding of what assets, systems and functions make up the sector; how these are interconnected with other infrastructure sectors; what vulnerabilities exist in the nation's information systems and networks; what threats they face; and how to avert them or mitigate current risk levels.

Authors of this report:

Eric Goetz (egoetz@ists.dartmouth.edu)
Research Analyst, IRIA

Input and assistance received from George Bakos, Julie Cullen, Trey Gannon, Robert Gray, Garry Kessler, Dennis McGrath and Brett Tofel.

[3] In this report I&T sector will be used to refer to the information and telecommunications infrastructure sector. A distinction must be made to IT, which usually stands for information technology.

Defining the Information and Telecommunications Sector

The term 'information and telecommunications sector' is widely used, but difficult to define exactly. The sector encompasses all systems and activities related to the exchange of electronic, voice, and image data via the Internet, telephones, satellites, and other communications media. The information and communications data that is central to this sector is used for myriad private, business, military, and government transactions on a daily basis, and society in its present form would cease to function without it.

- The President's Commission on Critical Infrastructure Protection (PCCIP) defines telecommunication infrastructures as follows: "The networks and systems that support the transmission and exchange of electronic communications among and between end-users (such as networked computers)."[4]
- LegalNetworks suggests: "The telecommunication infrastructure encompasses the computing and telecommunications equipment, software, processes, and people that support the processing, storage, and transmission of data and information."[5]

Despite the nation's acute reliance on these systems and functions, most of the I&T sector's assets (and those of most other critical infrastructure sectors), are privately owned and integrated into the public network.[6]

Convergence Toward a Next Generation Network

Presently, it still makes sense to talk about the public switched telephone network (PSTN) and the Internet as physically separate infrastructures. Each still operates separate communications backbones and networks, as well as switches and signaling and management systems.

In recent years, a revolution in the I&T sector has been witnessed that has resulted in traditional communications systems increasingly merging with Internet-based technologies toward what has been termed the Next Generation Network (NGN).[7] This evolution of communications from circuit- to packet-switched networks means that information networks and communications systems have become closely intertwined, and

[4] 'Our Nation's Critical Infrastructures – Working Definitions', President's Commission on Critical Infrastructure Protection (PCCIP) - http://www.info-sec.com/pccip/web/glossary.html
[5] LegalNet Works Telecommunications Infrastructure Definition - (link no longer active)
[6] "The public network (PN) is any switching system or voice, data, or video transmission system that is used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks)." 'An Assessment of the Risk to the Security of Public Networks', The Network Security Information Exchanges, National Communications System, Washington, D.C., December 12, 1995.
[7] The Next Generation Network (NGN) is a public, broadband, diverse, and scalable packet-based network evolving from the public switched telephone network (PSTN), Advanced Intelligent Network (AIN), and Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence. 'Convergence Task Force Report - Understanding Convergence and Interconnection of Emerging Networks – NGN Convergence: Security Issues and Recommendations', The President's National Security Telecommunications Advisory Committee, June 2001 - http://www.ncs.gov/nstac/ConvergenceReport-Final.htm

critical I&T infrastructures are becoming more reliant on IP services and the public Internet.

The I&T sector is rapidly transforming from relatively distinct and separate telephone (switched voice) and digital (IP-based packet data) networks to an interconnected network that delivers a plethora of services over a single network architecture. Traditional circuit-switched networks and Internet Protocol based data networks will coexist and interoperate until packet-based networks totally subsume circuit-switched networks. Eventually, some say in as little as 3-5 years, the I&T infrastructure will host the complete convergence of telephone, data and video networks into a single, packet-based architecture - a unified next generation network (NGN).[8]

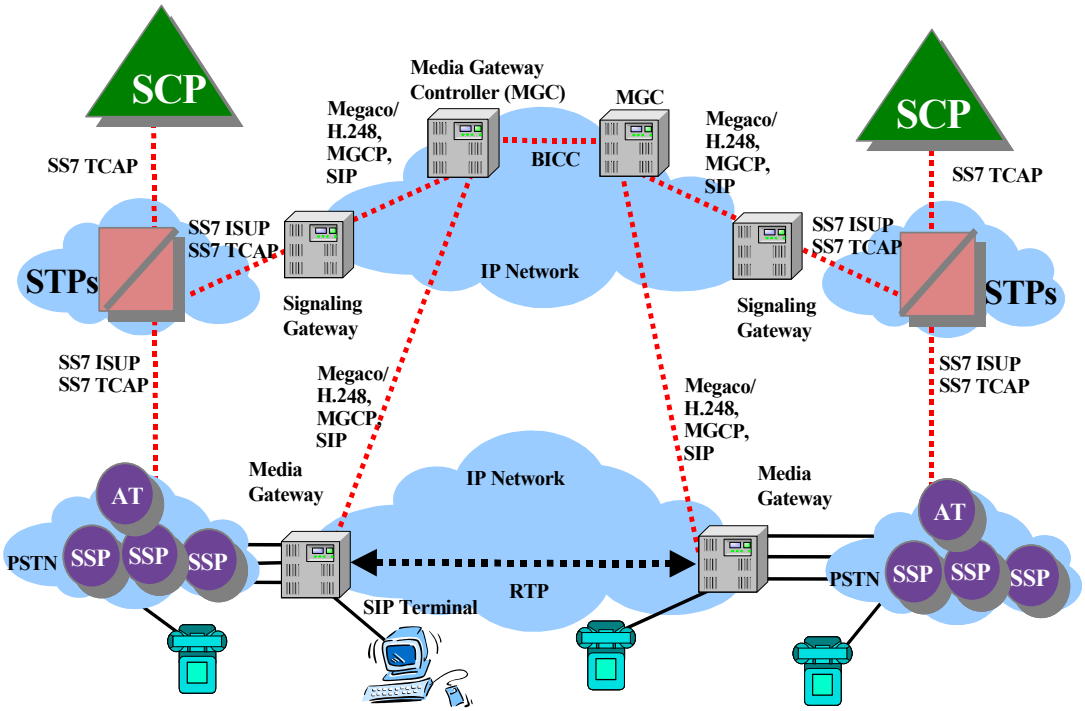

Fig. 1 - PSTN and NGN Convergence Architecture – Source: 'Network Security/Vulnerability Assessments Task Force Report', The President's National Security Telecommunications Advisory Committee', March 2002

The existing labyrinth of communications systems and networks is highly complex, combining different technologies, assets, applications, management systems and protocols in an expedient, but somewhat nebulous manner. The interconnections between voice and IP-based communications networks are not fully understood – assets are often shared or co-located and voice management traffic can run over, or be accessible from,

[8] 'A Step-by-Step Migration Scenario From PSTN to NGN – Technical Paper', Alcatel, January 3, 2002 - http://www6.alcatel.com/homepage/builder.jhtml?content=/publications/abstract.jhtml&repositoryItem=/x/articlepaperlibrary/vndmigration.jhtml and 'Convergence Task Force Report - Understanding Convergence and Interconnection of Emerging Networks – NGN Convergence: Security Issues and Recommendations', Op. Cit.,

the Internet. Further, myriad possible connections and network crossovers exist that could result in failures or cascading outages that cannot easily be predicted.

As mentioned, different communications traffic frequently utilizes the same assets or has assets co-located at the same physical locations. This is true for cables and switches in the 'first mile' – or 'local loop' – as well as for some backbone cables and communication nodes. For instance, at town or city districts the different kinds of landline and wireless communications traffic may come together at a local switching office or telco center – most traffic may also travel on cables owned by a single provider. Similarly, as fiber optic cables can transport various kinds of communications data, backbone cables often carry digital voice communications, voice-over-IP, or regular IP-based Internet traffic simultaneously.[9] Moreover, traditional voice communications currently rely heavily on software and digital data exchanges for crucial management functions, such as call setup. In addition to this technological convergence, international communications- and information networks are also merging, thereby more closely linking member countries together in a global I&T network. These international ties may also expose national infrastructures to vulnerabilities and outages.

Interconnections Between the I&T Sector and Other Critical Infrastructure Sectors

The I&T sector is crucial for the functioning of national and international political and economic systems.[10] Virtually every other infrastructure sector relies on the I&T sector for some vital operations. Each infrastructure's key assets are operated, monitored, or controlled by networked computers and other communication systems. The I&T sector is the information backbone that transports all this data. This crucial role in the proper functioning of modern societies makes the I&T sector a highly attractive target for physical or cyber attacks that could seriously disrupt communications and the free flow of information. Such disruption would invariably have a cascading ripple effect on other infrastructures, such as banking and finance, transportation, energy, water, government and emergency services.

As seen on September 11, 2001, a multitude of critical financial and business functions and systems were seriously disrupted for several days by the telecommunications outages

[9] Not all digital communications data must be IP-based – other protocols, such as NetBEUI, are used. Voice data is generally converted from analog to digital at the home or in the local telecom end office/switching office. It then travels across the wires as digital data (not necessarily IP-based). However, voice-over-IP services now exist in some markets that provide voice communications directly via the Internet. In this case, assets, systems and functions of voice and Internet communications are identical. In other instances, separate voice and Internet communications use the same physical cables and/or switching offices/telco centers, thereby creating critical communications nodes.

[10] A RAND report from 1998 identified energy production, telecommunications and computer-based systems as holding "an inescapable position of centrality…Thus, they are collectively of first priority for attention and remedial actions." 'The Cyber-Posture of the National Information Infrastructure', William H. Ware, RAND Corporation, 1998 - http://www.rand.org/publications/MR/MR976/mr976.html#pref

caused by the collapse of the World Trade Center and surrounding buildings.[11] The attacks demonstrated the delicate interconnections between different infrastructures and the manner in which localized attacks against critical communication nodes can have a global impact. A recent MARC transportation system computer glitch caused several hour delays in the Washington D.C. area, again highlighting how intertwined other infrastructures sectors are with the communications infrastructure.[12]

The reverse is equally true. Outages or attacks against other infrastructure sectors could have an effect on the unhindered flow of information and telecommunications data. For example, sustained attacks against the electrical power grid would shut down most forms of voice and Internet traffic in a matter of days, as most facilities have no power backups (or generators that last for a short period of time). The higher traffic volume trying to pass through fewer active cables, switches, and nodes would also congest the system to the extent of making it almost useless.[13]

> "Chain dependencies may produce unforeseen domino effects, whereby disruption of one infrastructure may spill over to other infrastructures. Coping with such domino effects will only be possible if the extent of the interdependence is clearly understood and if effective, well thought-through emergency preparedness measures have been taken. The fact that, in some cases, this interdependence transcends national boundaries constitutes an additional complicating factor." *('In Bits and Pieces – Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society', Ir. H.A.M. Luiijf and Dr. M.H.A. Klaver, Issue Paper for the 'Vulnerabilities in ICT-networks' Infodrome workshop in Amsterdam, March 2000)*

The recent Blue Cascades exercise highlighted infrastructure interdependencies and, particularly, other sectors' reliance on the I&T sector for vital operations. These relationships are often poorly understood and emergency responses are not adequately

[11] See 'Building a 21st Century Telecoms Infrastructure – Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations', Downtown Alliance, Association for a Better NY, NY Building Congress and the Real Estate Board of NY, August 2002 or 'Digital Destruction Was Worst Imaginable', Dan Verton, Computerworld, March 4, 2002 - http://www.computerworld.com/managementtopics/management/recovery/story/0,10801,68762,00.html

[12] 'Computer Problems Snarl MARC's Evening Rush', Lyndsey Layton, Washington Post, August 6, 2002

[13] A blackout in the Dutch province of Utrecht and surrounding areas on June 23, 1997, as a result of a combination of operational errors and technical malfunctions, produced a ripple effect with far-reaching consequences for the IT sector. "Such a blackout over a larger area would mean that ICT-infrastructures either cease to function or are exposed to serious congestion." See 'In Bits and Pieces – Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society', Ir. H.A.M. Luiijf and Dr. M.H.A. Klaver, Issue Paper for the 'Vulnerabilities in ICT-networks' Infodrome workshop in Amsterdam, March 2000 - http://www.tno.nl/instit/fel/refs/pub2000/luiijf_bitbreuk_english.pdf Also see 'Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks', Dr. Adam Cobb, Foreign Affairs, Defence and Trade Group, June 29, 1998 - http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm. It should be noted, however, that local power outages usually do not affect telephone services. National or regional power outages are a different matter.

planned.[14] More work needs to be done in this area to highlight infrastructure interconnections and dependencies, which will help decision makers plan for all contingencies. Attacks against information and telecommunications infrastructures can have national security and economic implications beyond the perceived boundaries of this sector. In addition, "Events in cyberspace can impact systems in physical space, and vice versa."[15] Hence, the consequences of an I&T sector attack need not be merely 'virtual' – tangible physical effects on people and objects can and will ensue.

Assets, Systems and Functions

No comprehensive inventory of the I&T sector's assets, systems and functions has been published, although work in this area is underway. In general, the sector encompasses all the assets, systems and functions related to the unhindered flow of information and other communications data via the Internet, landline and wireless telephones, satellites, fax machines and other communications media.

Assets

The I&T sector consists of a vast array of assets. A detailed inventory would need to list these assets specifically and classify them into different categories. This report will focus solely on generic types of assets. Assets for the I&T sector include:

- Entry/exit points
- Cables
- Switches/routers
- Communication nodes
- Management and control systems

Entry/Exit Points

Entry/exit points are essentially the gateways where communications data enters the various networks. For wireline voice communications traffic, telephones and other appliances offer network access. This traffic is generally transported to a local telco end office or central office. Wireless voice communications are picked up by antennas and sent to base stations. From these wireless cell sites, traffic makes its way to a local telco office, where it is integrated into other communications streams. Internet data enters the system through home or business client machines or networks. Home users generally

[14] The final report and executive summary for the Blue Cascades table-top exercise found that: "Organizations represented demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures, vulnerabilities, and operational dynamics of these regional interconnections, particularly during longer-term disruptions…There was little recognition of the overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans, and the need for contingency plans in the event of loss or damage to electronic systems." - 'Blue Cascades – Infrastructure Interdependencies Table-Top Exercise - Final Report and Executive Summary,' Pacific Northwest Economic Region, Partnership for Regional Infrastructure Security, July 18, 2002 – http://www.pnwer.org/pris/CascadesReport.htm

[15] 'The National Strategy to Secure Cyberspace – Draft Version', The President's Critical Infrastructure Protection Board, September 18, 2002 - http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf

gain access to an Internet service provider's (ISP) network through an ISP's point of presence (POP), [16] while companies usually have a direct link to the ISP's network. Many of these access technologies are used jointly by different services or assets are shared.

Cables

A wide variety of cables, or bundles of cables, are used to transport all kinds of information and communications data around the country. Phone lines from home users and businesses (especially in rural areas and small towns) to their local telco end office/ central office are often still made of copper. However, optical fiber cables are increasingly used for all types of communications traffic, as any service can run over them. Cables are used to connect end users with their local telco end office/central office in what is called the 'local loop' or 'first mile'. From there, other cables transport the data to larger switching offices and other communication nodes. Synchronous optical network (SONET) rings are widening rings of optical fiber cables (connected to individual switches) that ensure the robustness and redundancy of the system.[17] Backbones[18] are the central arteries that transport the vast amounts of voice, Internet and other communications data around the country. Separate backbones for voice and Internet traffic still exist to a certain extent, but some backbone cables carry both kinds. Often separate backbones run parallel to each other along the same routes, and converge at the same communication nodes.

Switches and Routers

Switches and routers are the intersections of the communications networks. All kinds of communications data are sent to their destinations via a variety of switches and routers. Voice traffic generally passes through a series of switches that connect different network nodes. This used to be done manually, but now digital voice data is often passed on with the help of virtual switches, using technologies such as Frame Relay (FR) or

[16] "A point-of-presence (POP) is an access point to the Internet. A POP necessarily has a unique Internet Protocol (IP) address. Your Internet service provider (ISP) or online service provider (such as AOL) has a point-of-presence on the Internet and probably more than one. A POP may actually reside in rented space owned by the telecommunications carrier (such as Sprint) to which the ISP is connected. A POP usually includes routers, digital/analog call aggregators, servers, and frequently frame relays or ATM switches." – whatis.com definitions: point-of-presence

[17] Synchronous optical network (SONET) rings ensure continued communications traffic flow, even if the line is severed or a node is taken out. Through the ring, traffic can be passed on in two directions; if one path is removed, the data can still reach its destination in the other direction. Therefore, a SONET ring must be severed in two separate locations to stop the flow of data. Such rings usually exist in and around a city or town and then again at the regional and national levels. **"**Despite the increased robustness provided by SONET rings, the very high capacity of fiber optic cables results in a greater concentration of bandwidth over fewer paths because of economic considerations. This means that the failure, or sabotage, of a single link will likely disrupt service for many customers." 'Trust in Cyberspace', Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, National Academy Press, Washington D.C., 1999 - http://www.nap.edu/books/0309065585/html/index.html

[18] Backbones are typically fiber optic trunk lines. The trunk line has multiple fiber optic cables combined together to increase the capacity.

Asynchronous Transfer Mode (ATM).[19] As voice communications require an end-to-end connection, each switch must maintain an open line between users for the duration of the call. Internet traffic is passed along by routers that send IP-packets to their destination via the most efficient route. Routers are the connection points between different Internet networks. As Internet traffic is connectionless, a router passes on data packets one at a time without requiring a sustained end-to end link.

Communication Nodes

Communication nodes are the points where different communication strands converge. In contrast to single switches and routers, communication nodes are taken to mean physical locations where a variety of cables and/or switching equipment/routers and/or management, signaling and control equipment come together. These crucial meeting points can bring together a variety of voice or Internet cables in a single location. They can also act as gateways between circuit-based PSTN and packet-based IP networks. Major Internet service providers exchange backbone traffic at network (national) access points (NAPs)[20] or private peering points.[21] Different types of communications data, including voice and Internet traffic, are often brought together at telco hotels and central switching offices.

Signaling and Control Systems

Signaling and control systems are also vital assets in the I&T sector. A number of signaling, management and control functions have to be performed to ensure the smooth information flow. Much of this activity for Internet and voice traffic is conducted along the same channels used for the communications data. Voice communications signaling and control data, however, is out of band and not directly accessible from outside the phone operator's network. The ITU-T Common Channel Signaling System 7 (SS7) network, for example, is responsible for communications between switches and other nodes.[22] Network Operations Centers (NOCs), where elements of a network (switches,

[19] For a good introduction of telecommunications systems and technologies see 'Telecom Crash Course', Steven Shepard, McGraw-Hill, 2002 or 'The Essential Guide to Telecommunications – 2nd Ed.', Annabel Z. Dodd, Prentice Hall PTR, 2000

[20] NAPs are communication nodes where all the national Internet service providers (ISPs), and major regional ISPs, exchange data at a single location. At first, only a few NAPs, such as MAE East and MAE West, existed; at present, there are thought to be between 50 and 100 of these NAPs (depending on definitions). For more information on the number and location of NAPs and other public data exchange points go to: http://www.ep.net/. With a few exceptions, NAPs are used to localize Internet traffic and minimize the dependency on international backbones. See 'NAPs, Exchange Points and Interconnections of Internet Service Providers: Recent Trends Part I: 2000 Survey of Worldwide NAPs and Exchange Points', Jeffrey Baker, ep.net, March 31, 2000 - http://www.ep.net/ep-rpt-sum.html. While important, NAPs are not the only links between major ISPs.

[21] Private peering points are nodes where two (or several) major ISPs exchange traffic directly. It is unclear exactly how many of these private peering points exist, but all major ISPs are known to swap traffic in this fashion. Any attack against these private peering points would require significant insider knowledge (the location of NAPs is well known). For more information on ISP peering practices see 'Internet Service Providers and Peering', William B. Norton, - http://www.cs.ucsd.edu/classes/wi01/cse222/papers/norton-isp-draft00.pdf

[22] "Common Channel Signaling System No. 7 (i.e., SS7 or C7) is a global standard for telecommunications defined by the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T). The standard defines the procedures and protocol by which network elements in the public

transmission lines, access devices, etc.) are monitored and controlled, are also crucial communication assets.[23]

In sum, the assets are all the hardware that, together, is needed to successfully transport and manage information and communications data.[24] Information and communications infrastructures frequently share assets (local loop, cable to headend, backbone cables, telco offices, switches, routers for voice-over-IP etc.) or have assets co-located at the same facility.

Systems

The I&T sector used to be comprised of two main meta systems: traditional circuit switched networks, mainly the wireline public telephone network, and packet-based Internet Protocol (IP) networks, primarily the Internet. These systems were at the apex of a vast hierarchy of sub-systems. A complex, "interdependent, diverse, circuit- and packet-switched network using terrestrial, satellite, and wireless transmissions systems to support voice, data, image, and video communications, supported primarily by software-based controls"[25] is currently in use. Although it still makes a certain amount of sense to view them as separate, if strongly interconnected, systems, this distinction is becoming increasingly blurred as the I&T infrastructure develops into a next-generation network.

Both the public phone system and the nation's Internet infrastructure consist of a complex hierarchy of service providers that interact with one another at different levels. No centralized authority exists, meaning that Autonomous Systems (AS) must cooperate with one another.[26] The Internet used to be structured as a hierarchical tier system with tier 1 providers at the pinnacle and hundreds of smaller ISPs extending downwards; now, a variety of nodes are peering directly horizontally, making the system more diffuse, distributed and redundant. However, a small number of highly connected nodes still exist that handle a large percentage of net traffic (See Fig.2).

switched telephone network (PSTN) exchange information over a digital signaling network to effect wireless (cellular) and wireline call setup, routing and control." - 'SS7 Tutorial', Performance technologies - http://www.pt.com/tutorials/ss7/. For more information on SS7, see 'Trust in Cyberspace', Op. Cit.,

[23] For more information on Network Operations Centers (NOCs), see 'Trust in Cyberspace', Op. Cit.,

[24] Some experts would argue that the people operating these information systems and the software used to manage them should also be counted as assets. This is especially true of the Internet, where firewalls, intrusion detection systems (IDS), proxies etc. could certainly be counted as assets. For the purpose of this study, assets will be used solely in reference to physical assets.

[25] The President's National Security Telecommunications Advisory Committee website - http://www.ncs.gov/nstac/attf.html#One

[26] About 14,000 autonomous systems (in this case registered autonomous networks) are believed to exist on the Internet at present. While no central authority exists, bodies such as the Internet Assigned Numbers Authority (IANA - http://www.iana.org/), the Internet Corporation for Assigned Names and Numbers (ICANN - http://www.icann.org/), the Internet Society (ISOC - http://www.isoc.org/) and the North American Network Operators Group (NANOG - http://www.nanog.org/) manage certain aspects of the relationships between autonomous systems.

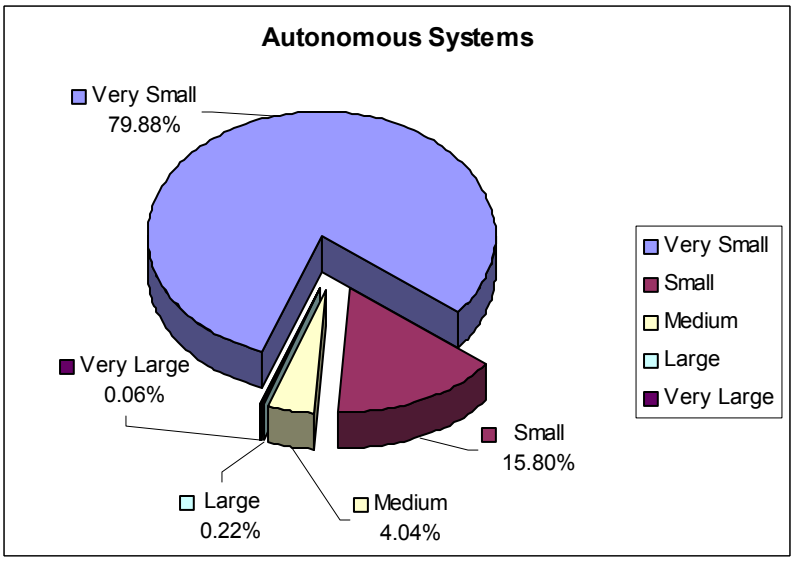

Fig. 2 - A Breakdown of Autonomous Systems by Number of Neighbors[27]

Network traffic volume is geographically concentrated, mainly along the U.S.'s east and west coasts (See Fig. 3). This Internet traffic concentration invariably leads to increased vulnerability points in the form of highly connected networks.

The public telephone network is more rigid and relies more heavily on individual components.[28] Yet the number of service providers – and route diversity and redundancy - has increased significantly in recent years. Again, this distinction is becoming more diluted as the public telephone network and the Internet increasingly merge and use each other's assets and sub-systems. Nonetheless, the wide variety of existing communications technologies and systems already often merge and have single vulnerability points – e.g. satellite or wireless communications often join wired voice or Internet networks and are transported through the same assets (cables, switches, nodes etc.). Service diversity is often solely at the local level.[29]

[27] Only a tiny number of Internet networks (0.06%) are very large (have 500 or more neighbors) and a further 0.22% are large (have between 100 and 499 neighbors) – almost 80% are very small and have only 1-3 neighbors. This means that a small number of networks carry a large proportion of global network traffic. See 'Internet Monitoring and Historical Route Archive using the Border Gateway Protocol: Progress Report August 2002', Dennis McGrath and George Cybenko, Institute for Security Technology Studies, August 2002

[28] According to the National Research Council "The PTN is structured around a relatively small number of highly reliable components. A single modern telephone switch can handle all of the traffic for a town with tens of thousands of residents; long-distance traffic for the entire country is routed through only a few hundred switches." 'Trust in Cyberspace', Op. Cit.,

[29] For a more detailed description of telecommunications systems and different communications media see 'The Internet's Coming of Age', Computer Science and Telecommunications Board, 2001 - http://bob.nap.edu/html/coming_of_age/

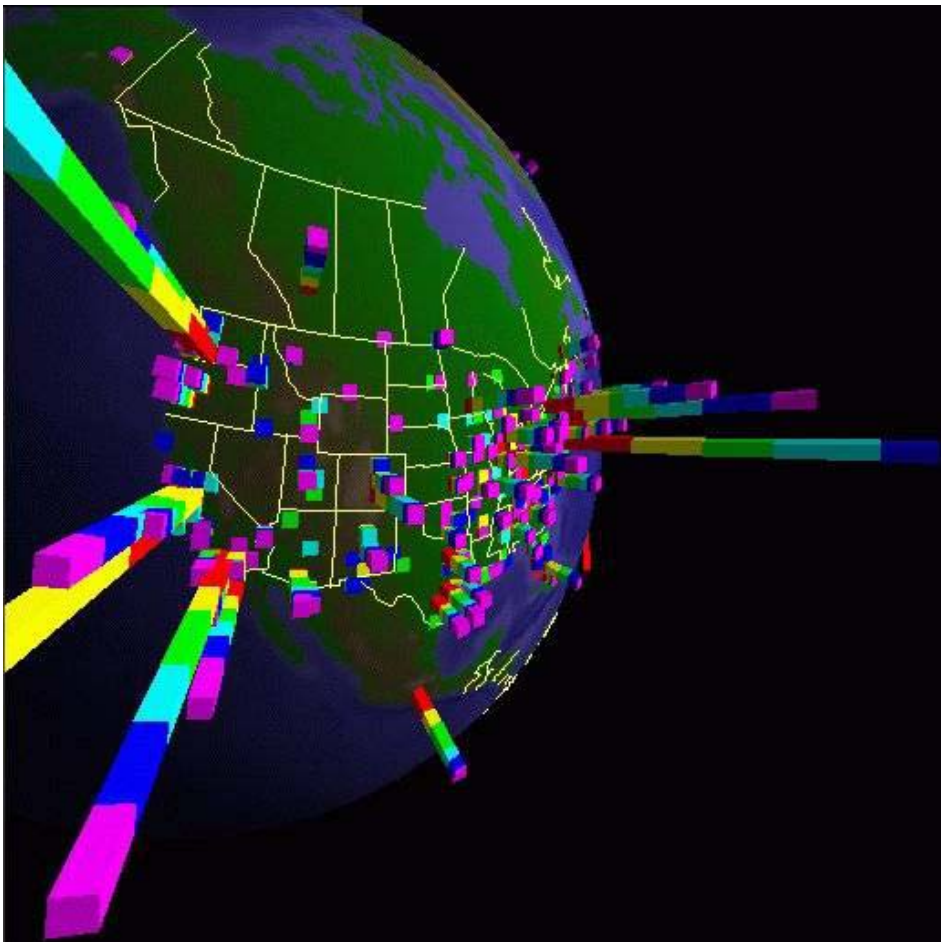

Fig.3 – Geographic Visualization of Web Traffic in the U.S. – Source: Department of Computer Science, University of Illinois

Functions

The I&T sector's functions are clear: to deliver vast amounts of voice, electronic, and image data to government and business organizations and the general public quickly, efficiently and reliably, while maintaining data confidentiality, integrity and availability. This function is crucial to the proper functioning of high-tech societies, yet the complexity of the systems that transport and manage this data has multiplied. At the lower levels, each system and sub-system, and each asset, has its own specific function to support the overall I&T sector function. Each cable, for example, has the function of transporting data, while switches and routers have the function of controlling data flow and direction.

Vulnerabilities

Overall, the I&T sector is relatively robust, diverse and redundant. It is well equipped to resist total devastation and even major outages.[30] Nonetheless, vulnerabilities exist,

[30] According to the Network Reliability Steering Committee, wireline telephone networks remained robust in 2001 and the first quarter of 2002. The overall number of outages reported was the lowest to date,

mainly in the form of critical communication nodes and systems.[31] These communications bottlenecks often coincide with concentrations of people and economic activity - mainly along the east and west coasts of the United States and around the great lakes – and are difficult to remedy.[32]

While nationwide communication failures appear unlikely, regional outages are a possibility. Although a variety of different information and communication providers and systems (voice, data, wireless, microwave, satellite etc) exist in most markets, these systems often rely on, and interact with, one another. Different systems often use the same resources (switches, cables etc.) to provide service, or co-locate critical assets in the same physical location. This creates single points of failure – at least at the local and regional levels – that makes the sector vulnerable to attacks.

Topology

The general structure of the Internet's networks is relatively well understood and documented (see Fig. 4).[33] Although the telephone network's topology is not as readily available, it should be noted that both networks often mirror one another. Either cables are shared for both kinds of communications data, or Internet providers utilize existing phone cable routes to lay cables for IP-traffic.

although Common Channel Signaling (CCS) outages were on the rise. See 'Network Reliability Steering Committee – Annual Report 2001', Network Reliability Steering Committee - http://www.atis.org/pub/nrsc/2001rpt.pdf and 'Macro-Analysis: First Quarter 2002', Alliance for Telecommunications Industry Solutions, Network Reliability Steering Committee, P.J. Aduskevicz, Chair, NRSC - http://www.atis.org/pub/nrsc/1Q02macanal.pdf

[31] See 'Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks', Op. Cit., for an excellent analysis of specific infrastructure sector vulnerabilities in Australia. Also, 'In Bits and Pieces – Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society', Op. Cit., provides a useful analysis or vulnerabilities in the Dutch IT sector with examples of past problems and outages. No similar open source document is available in the United States, but would be extremely valuable in helping to assess vulnerabilities and threats for the IT sector.

[32] 'Information and Communications Sector Input into the National Strategy for Critical Infrastructure Cyberspace Security', May 2002 - http://www.pcis.org/getDocument.cfm?urlLibraryDocID=32

[33] It should be noted that exact Internet network topologies do not exist as connections and paths change constantly and a significant percentage of these are not documented. However, a general topological overview, especially between major ISPs, can be provided. This overview further highlights system complexity.

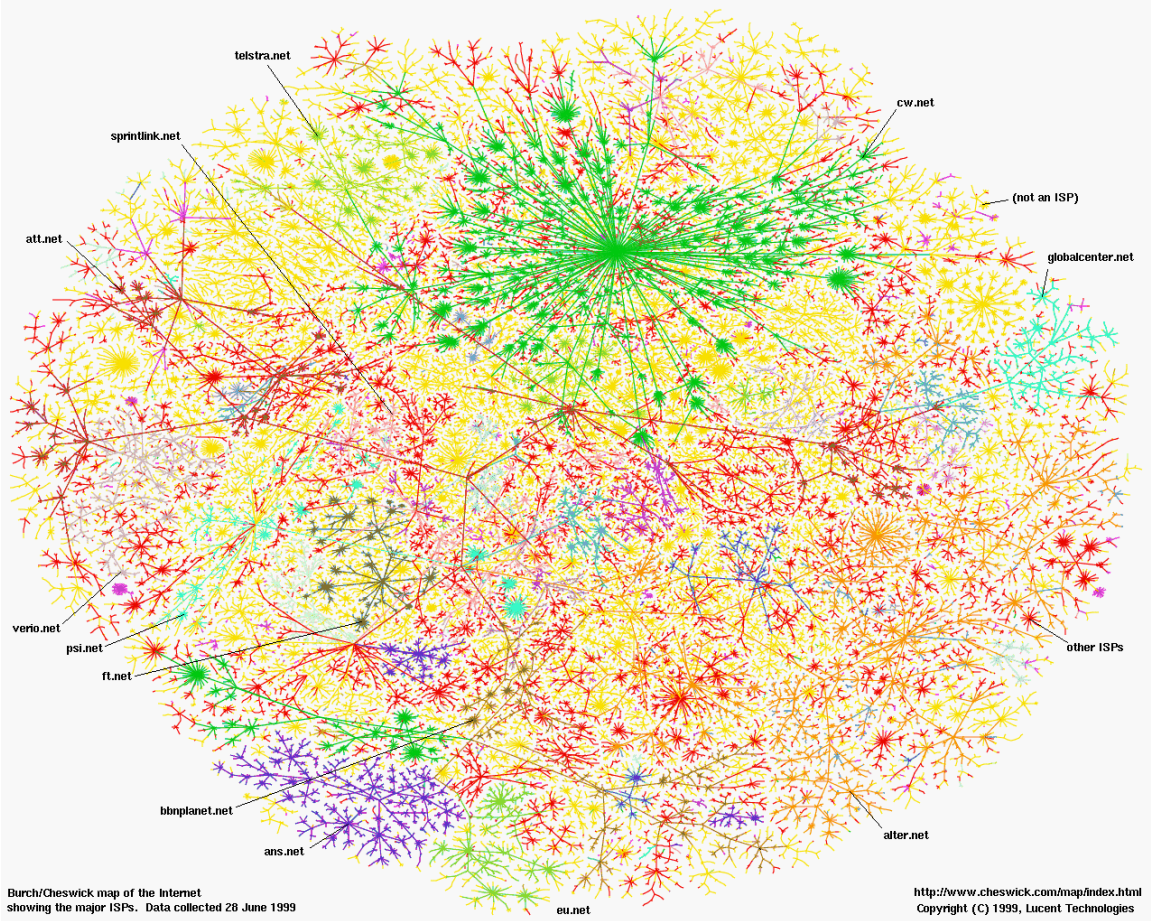

Fig.4 – Map of the Internet showing the major ISPs – Source: Courtesy of Lumenta Corporation. Patent(s) Pending & Copyright Lumenta Corporation 2002. All Rights Reserved.

Shared Assets

Tier 1 providers, like AT&T, WorldCom and Verizon, often transport voice and IP-based communications data over the same fiber optic cable. Voice-over-IP assets are shared for different services by definition. At the local level, 'first mile' links often transport different traffic types, particularly as service providers (voice and Internet) often rent resources, assets and facilities from one another.[34] Therefore, certain cables, especially in the 'local loop' and backbone lines, are points of vulnerability. In support of this argument, a recent report by the Computer Science and Telecommunications Board concluded that "sharing (multiplexing) of communications facilities means that it is increasingly difficult to provision physically diverse communications links between two

[34] This was the case in Manhattan. Most service providers rented cables and switching facilities from the local provider Verizon. Therefore, when the terrorist attacks on the World Trade Center damaged Verizon's central switching office and its cables, many other service providers in the area were also no longer able to offer services. This is particularly problematic as some companies realized that the back-up systems they had put in place using a second provider turned out to run through their first provider's cables and switching office, rendering both useless during the crisis. See 'Building a 21st Century Telecoms Infrastructure – Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations', Op. Cit., or 'Circuit-Switched Networks', Bill Scanlon, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,130672,00.asp

given sites. For example, two nominally different communications links, even when obtained from different providers, may in fact run over the same fiber, in the same fiber bundle, or in the same conduit, meaning that they are both vulnerable to a single physical disruption."[35]

Some cables are more critical than others. Cable concentration, across bridges or through remote areas, for instance, could be particularly vulnerable to accidents or attacks because they may be the only link between two points. Several media giants now offer both voice communications and Internet services, which makes them more susceptible to physical or cyber attacks to both services, as their assets and/or management systems are more likely to be shared. Nonetheless, cutting a single cable or bundle of cables could probably only cause local or regional outages; even then only some services would probably be affected. Nationally, no cable presents a single point of failure as redundancies are built into the system.

Critical Nodes

In addition to the cables themselves, critical communication nodes – the places where several or many cables meet and interact with other vital hardware – are also points of heightened vulnerability. Different communications data converge in the 'first mile'. This data generally arrives at a telco central office/switching office, where it is processed for further distribution on phone and Internet networks. Sometimes all data is transported together to a regional switching office. These telco offices/switching offices present a point of vulnerability as they handle large volumes of diverse communications data for which there is often no alternative route.[36] Additionally, ISP points of presence (POPs) can also be crucial communication nodes that can cause significant regional service outages.

At the national level, despite existing redundancies and diverse routing in communications networks, critical cables still have to meet somewhere and interact with other vital components. This is a further point of vulnerability. Voice and Internet traffic often shares facilities like telco centers/hotels and major switching offices. These facilities are crucial communication nodes as they house hardware and software from a variety of service providers and are a meeting point for numerous voice and Internet communications strands. An attack against one of these facilities could certainly result in local or regional outages, and could affect services on a larger scale.

Telco Hotels

Telco hotels are facilities, mainly in large cities, where most of the major information and communications service providers converge to place switching, routing, and control

[35] 'The Internet's Coming of Age', Op. Cit., Also see 'In Bits and Pieces – Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society', Op. Cit.,

[36] According to this media source: "In a physical attack, disabling communications in the U.S. would be a frightfully simple task because both voice and data traffic move through as few as four buildings in some cities, and many are far less secure than they probably should be. Take out the main central office, cable headend, telecom hotel and carrier-neutral peering point in a particular city, and all but the simplest Internet-based communications would be seriously disrupted." 'Telco Center', Max Smetannikov, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,128463,00.asp

equipment, and cable links.[37] They are used to establish a provider's presence in that area and/or to exchange data with other providers. The physical location of these telco hotels is not a secret, although information on the subject has recently been removed from the Internet. Nonetheless, cached versions of this information remain readily available. Telco hotels are significant communication nodes and are points of vulnerability; if damaged or destroyed, they could cause measurable disruptions, particularly at the local and regional levels.[38]

NAPs

Network (national) access points (NAPs) and private peering points are also crucial nodes for Internet traffic where different data arteries converge creating heightened vulnerability. Although the number of NAPs and peering points is growing, they remain crucial to the unhindered flow of Internet traffic and may be attractive attack targets. The physical location of NAPs is well known, while the location of private peering points is less clear. Identifying a large number of these would require insider knowledge. It should also be noted that, although NAPs only accommodate ISPs, voice communication links and other communication assets are often housed in or near the same facility for convenience. However, even taking out all the NAPs simultaneously would probably not bring Internet connectivity to a grinding halt due to the existence of the many private peering points where ISPs also exchange data.[39] Such an attack would cause significant congestion, though, as too much traffic would be forced to travel via alternative links.[40]

International Gateways

International communications gateways - such as MAE East in Dulles, Va. or MAE West in San Jose, Ca., or telco centers on the east coast where international voice traffic arrives via underwater (submarine) cables or satellite - are also crucial nodes that may be vulnerable. Although the exact location of international voice gateways is not common knowledge, a well-placed insider could reveal points of acute vulnerability. There are only a few major connection points to Europe or Asia that, if disabled, could seriously disrupt traffic, primarily because voice and Internet data are also often transported through the same link. However, some communications providers have private

[37] For more information on telco hotels, including services provided and security measures, see 'Tutorial on the Design and Construction of Local and Regional Exchange Facilities – Version 0.3', Bill Woodcock, Packet Clearing House, March 2001 - http://www.pch.net/documents/tutorials/ep-construction/ep-construction.html, 'Telco Building Boom', Telephony, September 11, 2000 - http://www.layerone.com/company/news/000911_Telephony.pdf and 'Carrier-class Telecom Hotels', Wave Exchange - http://www.carrierhotels.com/properties/waveexchange/pdfs/WaveExchange.pdf

[38] 'Telco Center', Op. Cit., It should be noted that Verizon's central switching office that was destroyed in New York City on September 11, 2001 was not a telco hotel by definition, although it functioned like one in many ways: it housed equipment that was used by several companies to provide a variety of communication services to customers in Manhattan.

[39] For more information on NAPs and private peering points see 'NAPs, Exchange Points and Interconnections of Internet Service Providers: Recent Trends Part I: 2000 Survey of Worldwide NAPs and Exchange Points', Op. Cit., or 'The Internet's Physical Layers', Russ Haynal - http://navigators.com/sessphys.html

[40] For speculation on the potential impact of attacks against NAPs or other major communication nodes see 'Telecom Industry Beefs Up Priority Wireless Access, Backbone Security', Dan Verton, Computerworld, September 9, 2002 - http://www.computerworld.com/securitytopics/security/story/0,10801,74076,00.html

international links for traffic that does not leave their network. These could be more widely utilized if other outages occurred.

Signaling and Control Systems

The network control space and media gateway controllers - the points where the public switched telephone network (PSTN) and packet-based IP networks interact via signaling gateways - are also vulnerable because an attack here could lead to disruption in both networks.[41]

> "IP networks could present those with malicious intent a 'back door' into the control space of the PSTN, which could enable malicious activities such as insertion of false Signaling System 7 (SS7) messages. If unauthorized parties gain access to a signaling gateway, they could disrupt or suspend its operations, alter its routing tables, or use it to forward false communications to other signaling gateways. Such activities could precipitate network disruptions and impact overall network reliability and availability." ('Network Security / Vulnerability Assessments Task Force Report', The President's National Security Telecommunications Advisory Committee, March 2002)

The Signaling System 7 (SS7)[42] network is out of band and not directly accessible from the Internet. SS7 messages are separate from the network that transports the actual communications traffic, but often are transported on the same line. An attacker could manipulate SS7 signals with the help of an insider, or by first breaking into a phone company's private network. This could give an attacker access to, or control over, the signaling network that controls the switching of voice communications. Additionally, deregulation has forced telephone companies to allow "essentially anyone to connect into SS7 networks for a modest fee ($10,000). SS7 is a system that was designed for use by a closed community, and thus embodies minimal security safeguards. It is now employed by a much larger community, which makes the PTN subject to a broad range of 'insider' attacks."[43]

Crucial voice switches and gateways for voice traffic exist and are vulnerable – again, local assets are less redundant, but would only cause local outages. The closer one gets to the national level, the more robust and redundant the system gets, but the more critical

[41] For more information see 'Network Security / Vulnerability Assessments Task Force Report', The President's National Security Telecommunications Advisory Committee, March 2002 - http://www.ncs.gov/nstac/NSVATF-Report-(FINAL).htm or 'The Internet's Coming of Age', Op. Cit.,
[42] SS7 is a family of protocols used for all telephone calls that transcend switch levels. They are used to send all service signals between telephone network switching points and other switches, as well as to databases that manage services and advanced features. SS7 services include: basic call setup, management, and tear down; wireless roaming, authentication and services; local number portability; toll free and toll wireline services; and enhanced call features such as call forwarding, calling party name/number display, and three-way calling. See 'SS7 Tutorial', Op. Cit.,
[43] 'Trust in Cyberspace', Op. Cit.,

communication nodes become. A successful attack against the signaling network at the national level could have cascading effects and cause serious outages.[44]

Internet routers are even more vulnerable in this regard because routing protocols "execute in-band with the communications they control."[45] Therefore, routing and control messages are accessible online and if communication links become saturated, these messages are dropped just like the communications traffic itself, making DoS attacks more appealing.

Command and control mechanisms used in the I&T infrastructure for inter-device communications and customer services are also a point of vulnerability. Both voice-over-packet and voice-over-IP services are at risk of exploitation through flaws in signaling and management protocols.[46] Most telephone networks are administered behind the scenes by Unix systems and complex software and databases are used for call set-up and advanced customer services. These factors increase cyber attack vulnerability.[47]

As more and more management and administrative functions are placed online and opened to remote access, they become susceptible to manipulation. This should be countered through the implementation of secure data transmissions and message authentication. Wireless networks and protocols are even less secure than wireline systems, especially concerning information security. This could allow an attacker unauthorized access to otherwise well-secured networks.

Attacks related to deficiencies in authentication of communications between different elements of the infrastructures and different systems, and buggy code used to control and manage these infrastructures, also represent serious vulnerabilities that could be exploited to give attackers access to vital control mechanisms or sensitive data.

Domain Name System (DNS)

The Internet's domain name system (DNS) may also be vulnerable to attacks. It represents a central point of failure, but, again, not a single point of failure. The DNS is the central repository for domain name information and is, therefore, vital to Internet operations.[48] Physical or cyber attacks against the top-level DNS servers could result in

[44] A successful attack against the signaling network could allow an attacker to take out a signaling node or gateway, or to manipulate the content or destination of signaling messages. 'Network Security / Vulnerability Assessments Task Force Report', Op. Cit., Vulnerabilities in the signaling network will also change as communications evolve toward a next generation network. Parts of the SS7 signaling network will be replaced by a packet-based equivalent with potential new flaws. See 'A Step-by-Step Migration Scenario From PSTN to NGN – Technical Paper', Op. Cit.,

[45] 'Trust in Cyberspace', Op. Cit.,

[46] 'Network Security/Vulnerability Assessments Task Force Report', Op. Cit.,

[47] 'Trust in Cyberspace', Op. Cit.,

[48] The Internet's domain name system (DNS) is the distributed, hierarchical global directory that translates names (urls) to numeric IP addresses. The top two layers of the structure are critical to Internet operation. 13 'root' name servers are at the top of the structure, followed by 'top-level domain' (TLD) servers, which are authoritative for '.com', '.net', etc., as well as the country code top level domains (ccTLDs) responsible for '.us', '.uk' etc. See 'Overview of Attack Trends', CERT Coordination Center, April 8, 2002 - http://www.cert.org/archive/pdf/attack_trends.pdf or 'Root Name Server Operational Requirements',

serious problems,[49] especially as several of these servers are located in the same place. A successful attack against the root servers could prevent new look-ups if domain name information is not cached locally, as new requests go up the address tree to the root servers. Taking out one or several of the root or top-level servers could cause serious congestions as the remaining servers become overwhelmed with requests. Moreover, DNS (or cache) poisoning could allow an attacker to insert false addresses into the DNS, which would lead to confusion and the inaccessibility of some sites.

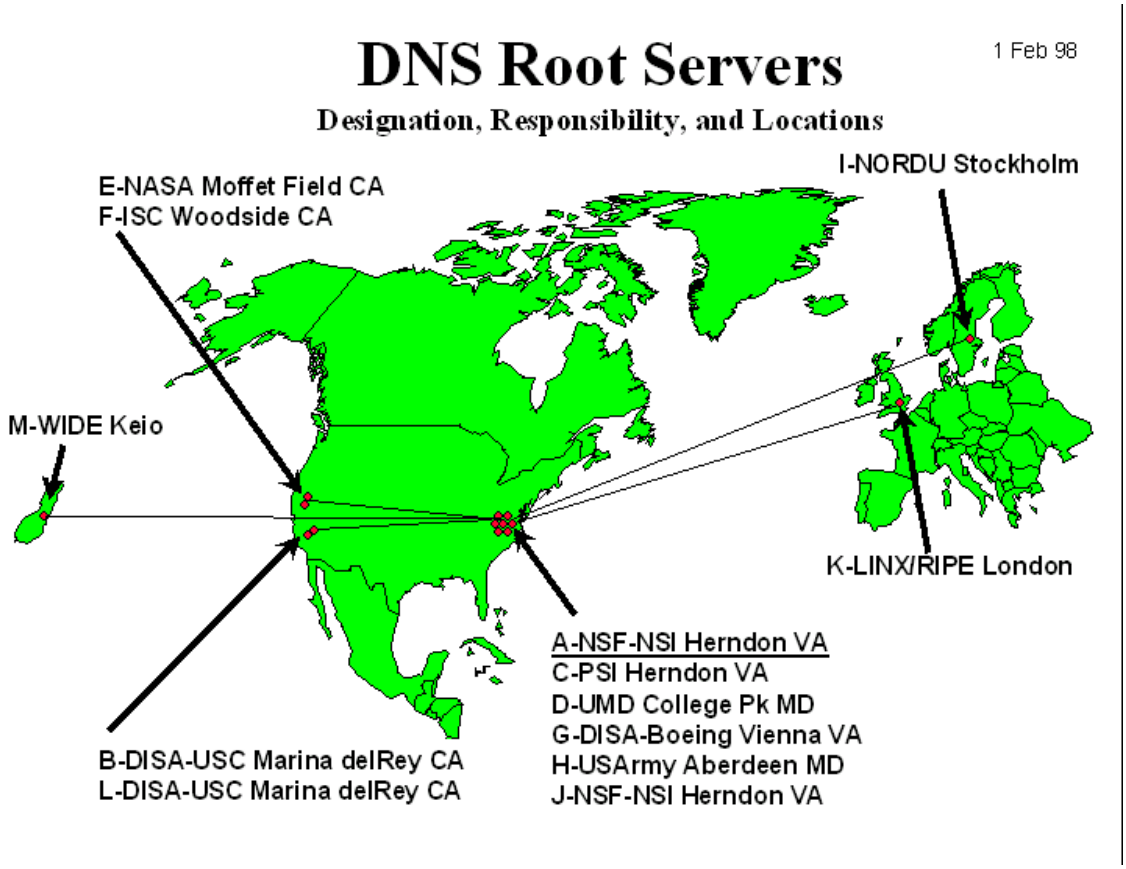

Fig.5 DNS Root Servers - Source: Internet Domain Name System Root Servers – World Internetworking Alliance (WIA) - http://www.wia.org/pub/rootserv.html

Network Working Group, The Internet Society, June 2002 - http://www.ietf.org/rfc/rfc2870.txt?number=2870 or The Internet Assigned Numbers Authority – Top-Level Domains - http://www.iana.org/domain-names.htm. For more information on how the DNS works, see Domain Name Service - http://www.scit.wlv.ac.uk/~jphb/comms/dns.html

[49] DNS servers using certain versions of Internet Software Consortium's Berkeley Internet Name Domain (BIND) server software have been found vulnerable, although not all the root or top-level servers still use BIND. See 'ICANN Panel Weighs DNS Vulnerabilities', Patrick Thibodeau, Computerworld, February 25, 2002 - http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,68588,00.html or 'Bind vulnerability threatens web hosts', vnunet.com, July 2, 2001 - http://www.vnunet.com/News/1120756 or 'Survey Results – Research on BIND Security', Men & Mice, March 2001 - http://www.menandmice.com/6000/6200_bind_research.html. Further, DDoS attacks against these servers may be successful in taking them out for sustained time periods. See 'Overview of Attack Trends', Op. Cit., or 'Icann warns of worldwide net threat', James Middleton, vnunet.com, November 14, 2001 - http://www.vnunet.com/News/1126863

However, several back-ups exist for these servers that can be put online relatively quickly, thereby minimizing the possible effects of an attack. Cached copies would also help keep the Internet functioning.

Telephone Networks

Fixed telephone networks are more centralized than Internet infrastructures and rely more heavily on a smaller number of assets.[50] The telephone system is more centralized and has less physical assets; therefore, these assets are better protected against physical (and cyber) attacks. According to a recent National Research Council report: "The PTN [public telephone network] is designed to have remarkably few switches, and it depends on them. That constraint makes it necessary to keep all its switches running virtually all the time."[51] "The result is a system that may not be robust in all circumstances, because if a critical component of the PSTN fails, the system fails."[52] If some of these critical components were damaged or destroyed, then this could cause significant outages.

The Internet

While the Internet is more dynamic and redundant than wireline phone networks, data on the Internet is more vulnerable - in transit and when stored on server and client machines - as few authentication measures and security safeguards are consistently deployed. As the same network is used for forwarding the communications traffic and for network management, the network elements are at risk of intrusion. However, phone networks are also increasingly relying on software and IP-based communications to manage systems and services, making them equally vulnerable to intrusions. Online systems have repeatedly been found vulnerable to various forms of malware (worms, viruses, Trojans) and cyber attacks, such as denial of service (DoS) attacks and unauthorized intrusions (hacking).

No Single Point of Failure

The I&T sector has no single national point of failure. No individual critical communication node exists that, if taken down, would cause serious nationwide outages/failures. Nonetheless, critical communication nodes exist where different forms of communications data converge or key arteries for voice or Internet traffic come together. Single points of failure only exist up to a certain level (local or regional).

Any communications asset could be a critical node if no redundancy for that particular asset is built into the system. A distinction needs to be made between assets at the network's edge and assets at the network's core. Assets at the network's edge may have

[50] This statement needs to be qualified. The phone network is not rigid and offers path re-routing if infrastructures are damaged as switches are normally configured with secondary and tertiary routes that can be used if primary links fail or become congested. Individual calls are not connectionless, so they would be lost, but the system as a whole can utilize a variety of routes to and from specific destinations. Voice telecommunications data is still less path redundant and dynamic than Internet traffic.
[51] 'Trust in Cyberspace', Op. Cit.,
[52] 'The Internet's Coming of Age', Op. Cit., "Furthermore, technical innovations, such as fiber optics and wave division multiplexing, enable fewer physical links to carry current levels of traffic. The result is a telephone network in which failure of a single link can have serious repercussions." 'Trust in Cyberspace', Op. Cit.,

less redundancy, but disabling that asset would only have local or, at best, regional effects. The closer an asset gets to the core, the more likely it is to be redundant. However, the closer an asset is to the core, the more critical it becomes – larger network and service outages become a possibility unless alternative routes are built into the system. Once the Internet backbone or the main (national) PSTN network is reached, redundancy and alternative routes are a given. This redundancy is due in part to the fact that the system was built to be robust and because there is currently a diversity of providers. However, if market consolidation were to occur in the telecommunications sector (perhaps due to bankruptcies during an economic downturn), more single points of failure may emerge.[53]

Even if no single I&T sector point of failure exists, a coordinated and well-timed attack against several critical nodes could cause significant damage. This point will be dealt with in more detail in the 'threats' section of this document.

Growing Complexity

The growing complexity and interconnectedness of I&T infrastructures means that the system as a whole, its assets, systems and functions, and the vulnerabilities it contains, as well as the potential for cascading effects and spill-over into other areas, are not well understood or documented.[54] As is pointed out in a recent National Research Council report, "The vulnerabilities of the PTN and Internet are exacerbated by the dependence of each network on the other."[55] This problem will be amplified when all communications merge as part of the next generation network because an attack against a router or other crucial system component will invariably affect all forms of communications traffic.

The diversity of services and the diffusion of assets would currently mitigate a total failure of the I&T sector. Temporary regional or local outages, or outages in specific communications services, are a more realistic scenario. This could still be significant if a particularly vital communications node (or several nodes) was targeted, or an attack took place at an inopportune time, such as in conjunction with other terrorist strikes or military conflict.

---

[53] Foreign ownership of information and telecommunications carriers and service providers is another issue worth examining. If too many of these crucial systems were in foreign ownership, would this have a negative impact on the flow of vital data, especially in times of crisis? At present, government regulation and oversight seems to be effective in averting this vulnerability, but the problem should be kept in mind. See 'The NSTAC's Response to the National Plan', The President's National Security Telecommunications Advisory Committee, April 2001 - http://www.ncs.gov/nstac/NationalPlanReport-Final.htm for a discussion of these issues.

[54] Much of the software that runs IT networks is so complex that it cannot be thoroughly tested and companies using it often do not know exactly how it will interact with other tools and technologies. A phone network outage suffered by AT&T on Martin Luther King's birthday in 1990 is an excellent case in point. A minor failure caused a switch to execute a piece of code that hadn't been tested. The software was missing a semi-colon, which caused the switch to fail. The failure rippled upstream causing neighboring switches to fail, until AT&T's entire long distance network was down. See 'AT&T Crash Statement: The Official Report', RISKS-LIST: RISKS-FORUM Digest, Forum on Risks to the Public in Computers and Related Systems, Volume 9:Issue 63, January 31, 1990 - http://www.infowar.com/iwftp/risks/Risks-9/risks-9.63.txt

[55] 'Trust in Cyberspace', Op. Cit.,

Examples of Infrastructure Damage

September 11, 2001

The terrorist attacks in New York City on September 11, 2001 serve as a sobering case study when analyzing I&T sector vulnerabilities because they caused catastrophic damage to some of the country's most critical communication nodes. The collapse of 7 World Trade Center onto Verizon's central office at 140 West Street caused significant telecommunications outages in Lower Manhattan – one of the world's most pivotal economic and financial centers. Specifically, 4 million high-speed access lines, 1.5 million circuits and over 100 fiber rings were damaged or destroyed as a direct result of the attack. 10 Verizon cellular sites were also destroyed, as well as AT&T's central office at 2 WTC.[56] Verizon offered no central office redundancy in this area as part of its standard service and most other communications firms leased Verizon's fiber optic cables to provide services in lower Manhattan. Therefore, almost every provider in the vicinity suffered full or partial loss of service.[57] Wireless disruptions and congestion were also experienced.

This incident highlights the vulnerability of critical communications systems to massive physical attacks, but also illustrates the remarkable resiliency of the I&T infrastructure. Some services, such as instant messaging and direct connect features, worked despite the devastation; most others were restored in a matter of hours or days through the application of back-up or emergency assets. Even this worst-case scenario was 'only' able to cause relatively short communications outages at a regional level.

Communications outages were relatively short and generally confined to the area, but had a wider operational, financial and psychological impact. Operationally, the communications outages complicated the crisis as emergency managers and first responders were unable to communicate. Furthermore, the world economic and financial system suffered immeasurable monetary losses following the terrorist attacks through lost business and loss of confidence in the financial system. Finally, the terrorist attacks in general, and the ensuing communications outages in particular, robbed the American public of its sense of security and the feeling of inviolability of the U.S. mainland.

While this report focuses primarily on the overall vulnerability of, and threats to, the information and telecommunications sector, the operational, financial and psychological effects of any attack against the sector should always be taken into consideration. For example, although the 2001 Code Red and Nimda worms did not threaten the functionality of the I&T sector as a whole, they are estimated to have caused billions of dollars in damages, lost productivity etc.

---

[56] 'Digital Destruction Was Worst Imaginable', Op. Cit., Also see 'Information and Communications Sector Input into the National Strategy for Critical Infrastructure Cyberspace Security', Op. Cit., for a list of damaged assets. It appears that, in addition to Verizon and AT&T, Earthlink, Sprint PCS, Cingular Wireless and WorldCom also lost communications equipment in the attacks.

[57] 'Building a 21st Century Telecoms Infrastructure – Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations', Op. Cit., or 'Attacks in New York provide sobering lessons', Mike Fish, CNN, January 5, 2002 - http://www.cnn.com/SPECIALS/2002/prepared.cities/stories/new.york.html

Baltimore Train Accident

The July 2001 train accident in Baltimore's Howard Street tunnel is also a good example to illustrate possible communications vulnerabilities. The accident damaged fiber optic cables used by seven of the country's largest Internet service providers to exchange data between networks. The damage to the physical infrastructure led to disruptions (Internet and even cell phone service was affected) felt as far afield as Africa.[58] The disruptions were initially blamed on the Code Red worm that was then propagating.[59] This incident again shows the vulnerability of crucial communication nodes to physical attack and underlines the mutual dependency of various communications systems. Here, a local event resulted in regional outages and even international disruptions of service.

Accidents, Flaws and Errors

The most common cause of communications outages in the past has been physical damage to cables during construction work, [60] other accidents, hardware or software flaws, or user errors. The I&T sector remains vulnerable to such occurrences. Similarly, computer glitches (such as the one that disrupted MARC service in the D.C. area), software flaws, and programming errors could suspend critical services.

Threats

Physical or cyber attacks could be launched against I&T infrastructure components - in stand-alone attacks or in conjunction with other terrorist strikes - to cause maximum damage and disruption. Hostile nation-states, perhaps in league with terrorist organizations, pose the most significant threat to the I&T infrastructure. Only nation-states really have the capabilities, intelligence and resources to launch a coordinated, large-scale attack against infrastructure components that has the potential to cause significant nationwide outages. Timing is crucial. The aim may not be to take out communications capabilities, but to gain prestige, or to cause a diversion (buy time through disruptions) during another crisis or military conflict involving the U.S.

Physical Attacks

At present, physical attacks against critical communication nodes or assets, such as backbone cables, telco hotels, switching centers or NAPs, are by far the greatest I&T infrastructure threat. These strikes could be perpetrated using bombs or explosives, or other more innovative weapons. Physical attacks are most likely because they require minimal skill and resources and because communication nodes and assets are relatively easy to physically damage.[61] Even so, due to built-in system redundancy, national

[58] See 'Tunnel Burns, Internet Melts', Michaela Cavallaro, The Industry Standard, July 20, 2001 - http://www.thestandard.com/article/0,1902,28110,00.html or 'Fire's effects ripple onto the Net', Sandeep Junnarkar, C-Net news, July 19, 2001 - http://news.com.com/2100-1033-270217.html

[59] 'Code Red 'was never a threat'', Mark Ward, BBC News, August 2, 2001 - http://news.bbc.co.uk/2/hi/sci/tech/1470246.stm

[60] Construction activity resulting in damage to fiber optic cables is believed to be the factor responsible for more than 50% of telecommunications facility outages. 'Trust in Cyberspace', Op. Cit.,

[61] 'The Cyber-Posture of the National Information Infrastructure', Op. Cit.,

outages or catastrophic system failures would be difficult to achieve.[62] Local or regional outages through attacks against switching offices or local provider central offices, or against crucial Internet or phone cables, are a more realistic threat.

However, a well-coordinated and timed simultaneous attack against several key nodes or assets could result in palpable service outages or disruptions. If a determined attacker launched a major physical strike against half a dozen well-chosen communication nodes (maybe in areas of geographic concentration, such as the U.S.'s eastern seaboard), this could lead to complete regional outages of some services for a short period of time, as well as more sporadic national and international outages and disruptions. Taking out pivotal gateways could also disrupt international communications links.

Electro-Magnetic Pulse (EMP) / Radio Frequency (RF) Fields

The possibility of an electro-magnetic pulse weapon being used against I&T infrastructures should be considered. Such an attack – however unlikely - could result in anything from temporarily disrupting telephone conversations "to the melting of components in every type of electrical system." [63] High power electro-magnetic fields also "pose a threat to critical infrastructures that depend on electronic equipment, such as public and private telecommunications networks."[64] Such attacks, using high power radio frequency (RF) fields, could endanger telecommunications switching stations or wireless base stations at the local or regional level, but a "full nationwide system collapse is not envisioned as a possible scenario."[65] Safeguards against these kinds of attacks are relatively widespread, but numerous critical communications assets remain vulnerable.[66]

Cyber Attacks

From a mid- and long-term perspective, cyber attacks also pose a serious threat to the I&T infrastructure.[67] As the sector becomes more diffuse and distributed and moves

[62] This point of view is reinforced by a recent U.S. government report: "Although physical security of critical communications facilities is essential, the effects of a physical attack are mitigated by the presence of multiple, diverse facilities-based networks. This alleviates the impact of communications disruption at an affected site and makes it unlikely that any single point of failure would cause regional or national disruption." 'Network Security / Vulnerability Assessments Task Force Report', Op. Cit., A study from Australia says: "The fact is that…the incredible array of systems and their myriad interlinkages that comprise the NII [National Information Infrastructures] provide a form of security in their very diversity. It would not be possible to completely disable these systems without detailed knowledge of their weaknesses and the location of critical nodes within and between them. Then only a well timed and coordinated strike might have a total effect." 'Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks', Op. Cit.,

[63] 'America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse', Jack Spence, The Heritage Foundation, May 26, 2002 - http://www.heritage.org/Research/MissileDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=12840

[64] 'Institute for Telecommunication Sciences 2001 Technical Progress Report', Donald L. Evans, Secretary, Nancy J. Victory, Assistant Secretary for Communications & Information, U.S. Department of Commerce, January 2002 - http://www.its.bldrdoc.gov/tpr/2001/

[65] Ibid.,

[66] Ibid., or 'America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse', Op. Cit.,

[67] According to the President's National Security Telecommunications Advisory Committee task force on network security and vulnerability assessments, "In addition to the enduring physical threat to the Nation's

toward a unified next-generation network, the number of vital communication nodes will increase, and an attack against a single node (or several nodes) will be less effective. Further a packet-based communications infrastructure for voice, data and image services will be more resilient to physical attacks because data can be dynamically re-routed around damaged system components. This development will make cyber attacks more appealing.

As cyber attack tools and techniques mature, it could become easier to take down worldwide communication systems. Future cross-platform computer worms could be utilized, perhaps in combination with logic bombs, denial of service attacks and other attack methods, for this purpose.[68] Next-generation worms, which combine a variety of attack techniques and propagation methods, and can be remotely controlled and updated, could target voice and IP-based communications – either directly or through corporate desktops that act as the interfaces for critical control and management functions. These worms could either act as denial of service (DoS) agents by flooding networks with traffic, or they could provide an attacker with unauthorized access to control systems. DoS or DDoS attacks in general remain a significant threat to IP-based communications systems.

Key communication nodes, such as core routers or DNS servers, could be targeted by such cyber strikes. Cyber attack methods are all the more dangerous because they are anonymous and cheap, can be implemented remotely, and automated attack tools are available online. Cyber attacks could be utilized to take control of and misuse crucial switches or routers (or other assets) for malicious ends, such as re-routing important communications data or launching DoS attacks against other systems. This could have more widespread consequences if the attack resulted in problems cascading through communications networks.

Future cyber attacks against I&T systems could take any number of forms and make use of emerging technologies. The constant discovery and cyclical patching of new vulnerabilities means that there are always a large number of unpatched systems on the Internet – this will become a more serious problem if software firms become entrenched as monopoly providers of operating systems (OS), servers or other key software. Peer to peer (P-2-P) tools, such as file-sharing software or business applications, could also become a new mechanism to spread malware or deliberately target vulnerable systems.

Hack attacks using social engineering also pose a realistic threat to the I&T sector. A skilled attacker utilizing telecommunications jargon, and with knowledge of an organization's structure and senior personnel, could gain access to vital management or control systems.

networks, cyber attacks present a growing threat to the security of U.S. information systems." 'Network Security/Vulnerability Assessments Task Force Report', Op. Cit.,

[68] A cyber attack simulation at the Summit Exploring Cyber Terrorism (SECTOR5) in Washington D.C. on August 21, 2002 provided such a scenario with present-day attack capabilities. Future cyber attack tools will be more sophisticated and effective as terrorist organizations and nation-states devote more resources to their development in an age of asymmetric warfare. See 'Cyberterrorism Scenario Scrutinized', Gretel Johnston, PC World, August 21, 2002 - http://www.pcworld.com/news/article/0,aid,104271,00.asp

Protective Measures

Defense in Depth

I&T providers and operators should embrace the concept of defense in depth. This means that security should cover multiple layers, including application, network, and perimeter security. If one layer is breached, additional security measures are in place. It is too often assumed that a single defensive layer, such as a firewall or IDS, will provide adequate security. Companies must supplement these tools with other security technologies, such as anti-virus software and/or honeypots, and protect systems and information at various levels. Defense in depth also implies the assumption that anything could happen. For instance, many management and control systems or critical nodes are not properly secured because they were designed to be separate from publicly accessible networks. However, as more and more of these systems are connected to the Internet, or other potential attack avenues open up via a company's private network, vulnerabilities invariably emerge.[69] Moreover, security requires greater diversity in software products. If a single firm gains a monopoly in any area, more systems will become vulnerable to a single type of attack.

Redundancy – Minimize the Number of Critical Nodes

On the national level, the best way to protect I&T infrastructures is to attain greater redundancy in I&T services and providers, and minimize the number of communication hubs, data bottlenecks and single-point-of-failure assets. Creating this physical, geographic and service diversity would undoubtedly make the I&T sector more robust and resilient.[70] Supporting the development of dynamic networks (IP networks), where possible, that can re-route data around damaged components would also help to reduce risk.[71]

The September 11, 2001 attacks on New York City illustrated the necessity of local or regional diversity and redundancy. Especially 'first-mile' redundancy is essential in order to secure service. Several providers should maintain multiple access routes and various backup methods for critical facilities, including the use of diverse communication systems (wireless, satellite etc. in addition to wireline systems). In the case of New York City, installing additional points of entry, duel carrier-neutral risers, and wireless

[69] See 'Security requires 'defense in depth', AT&T researcher says', Loring Wirbel, CommsDesign.com, September 10, 2002 - http://www.commsdesign.com/story/OEG20020910S0011

[70] Use of satellite communications internationally and within the United States could be expanded to provide reliable communications when assets are attacked. 'Satellites in Today's Internet – White Paper', Kul Bhasin and Eric A. Bobinsky, Workshop on Research Directions for the Next Generation Internet, Vienna, VA, May 13-14, 1997 - http://www.cra.org/Policy/NGI/papers/bhasinWP

[71] A recent report by the Network Reliability and Interoperability Council found that one key lesson from the September 11, 2001 terrorist attacks should be that: "Providers and customers should consider the benefits of redundancy and physical or geographic diversity, and deploy networks that can route voice and data traffic around trouble spots," 'The Future of Our Nation's Communications Infrastructure – A Report to the Nation', Network Reliability and Interoperability Council V, January 4, 2002 - http://www.nric.org/pubs/nric5/reporttothenation.doc

contingency systems on the roofs of some of Manhattan's commercial buildings, could have prevented some communications outages.[72]

The Government Emergency Telecommunications Service (GETS) program already "supports federal, state, and local government, industry, and non-profit organization personnel in performing their National Security and Emergency Preparedness (NS/EP) missions"[73] by providing them with priority communications access in times of network congestion or outages. Following September 11, 2001, over 10,000 GETS calls were made in New York City and Washington D.C. with over a 95% success of completion rate.[74]

Physical Security

All cyber security measures should go hand in hand with improved physical security of critical communication assets and nodes. This could be in the form of better perimeter security for buildings housing communications junctions, and improved access controls for physical assets and data systems, perhaps using biometric or other authentication technologies. In addition, the possibility of insider attack should be taken seriously and defended against through background checks and vigilance.

Awareness and Training

There is a need for better security education and awareness for developers, users and infrastructure operators.[75] Poor password policies, improper use of security technologies, badly configured systems, and general ignorance of security problems are still endemic despite warnings from government and private sector entities. Through programs to further awareness and security training courses, the general level of security will improve in the I&T sector.

New Protocols and Standards

The introduction of new security standards and protocols, like Internet Protocol version 6 (IPv6), Internet Protocol Security, and the Emergency Telecommunications Service scheme, would help secure information systems and data.[76] Additionally, risk of attacks could be minimized by using IPSec for secure, authenticated communications in operational systems used in the deployment, management, and provisioning of telecommunications infrastructures and where there is interaction of shared infrastructures (i.e., SS7).[77] Network perimeter security, through the use of intrusion

[72] 'Building a 21st Century Telecoms Infrastructure – Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations', Op. Cit.,
[73] 'The Government Emergency Telecommunications Service (GETS) program' - http://gets.ncs.gov/. Also see 'Telecom Industry Beefs Up Priority Wireless Access, Backbone Security', Op. Cit.,
[74] 'Exploring Solutions for Communications Reliability', National Communications System, Fiscal Year 2001 - http://www.ncs.gov/pdf/ncs_fy2001_report.pdf
[75] 'The National Strategy to Secure Cyberspace – Draft Version', Op. Cit.,
[76] See 'Network Security/Vulnerability Assessments Task Force Report', Op. Cit., or 'Security in the Traditional Telecommunications Networks and in the Internet', Markus Isomäki, Department of Computer Science, Helsinki University of Technology, November 29, 1999 - http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/tradsec/security_comparison.html
[77] 'Network Security/Vulnerability Assessments Task Force Report', Op. Cit.,

detection systems (IDS) and signaling gateway firewalls, would also add a measure of security wherever control data transits non-private networks.

New Technologies – Research and Development (R&D)

New technology utilization and the adoption of advanced security standards and protocols would improve the I&T sector's security and resiliency. Greater government coordination and funding of communications security efforts, as well as enhanced cooperation with the private sector, would also be beneficial. The draft version of the 'National Strategy to Secure Cyberspace' calls for enhanced federally funded and/or coordinated research and development (R&D) into tools and technologies to help identify vulnerabilities and cyber threats. R&D activity should be prioritized to meet the most serious near-term challenges, as well as planning for mid- and long-term technology needs at a time when I&T systems are undergoing profound changes.[78]

Text messaging and direct-connect features helped overcome the communications impasse in parts of Manhattan and at the Pentagon on September 11, 2001.[79] Furthermore, Free Space Optics[80] and others technologies have been discussed as ways to make the I&T sector more robust and diverse. The AscendentCOG technology, developed by Ascendent Telecommunications Inc., promises seamless communications in case of outages and disruptions - even if part of the system is destroyed – through the use of remote emergency facilities and wireless remote devices.[81] Additional R&D efforts could be directed toward self-healing systems, biometrics technologies or better encryption schemes, among others. Research is ongoing in a number of areas that could contribute to more secure communications infrastructures.

Conclusions

Overall, the I&T sector is fairly resilient, robust and redundant.[82] A variety of different communication methods and systems exist in parallel, so if one system is taken down, others can pick up overflow. Electronic data traffic, which increasingly underlies all forms of communications, is robust because, if one communications node is destroyed, traffic is simply re-routed. This makes it almost impossible to completely take down the Internet. Voice communications also possess a certain level of redundancy that allows alternative routes to be adopted if specific links or nodes are damaged.

---

[78] 'The National Strategy to Secure Cyberspace – Draft Version', Op. Cit.,
[79] 'Text Messaging to the Rescue', Alex Daniels and Brendan Barrett, Washtech, September 25, 2001
[80] Free Space Optics enables an organization to transmit data, at near gigabit speed, over a modulated beam of light from one point to another. 'Building a 21st Century Telecoms Infrastructure – Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations', Op. Cit., For more information on Free Space Optics see 'Tutorial on Free Space Optical Communications', Office of Engineering and Technology, Federal Communications Commission (FCC), September 16, 2002 - http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-02-2291A1.txt
[81] 'New system keeps phone lines open', Dibya Sarkar, Federal Computer Week, September 18, 2002 - http://www.fcw.com/geb/articles/2002/0916/web-phone-09-18-02.asp
[82] For a detailed examination of the reliability and robustness of the PSTN and the Internet see 'The Internet's Coming of Age', Op. Cit.,

Relative diversity of vendors and products for hardware and software for infrastructure components exists; therefore, targeting a single system or product cannot severely disrupt communications. If service is disrupted, the distributed nature of the Internet enables quick recovery. This makes the likelihood of an attack that causes sustained international, national or even regional disruption small.

However, a well-timed attack on specific communication nodes or assets could be used strategically to magnify the effects of other actions, or to cause economic or psychological harm. A determined enemy with extensive planning capabilities and resources could target several or many critical communication nodes at the same time in a coordinated strike. Such an attack – if successful – could have serious consequences, such as total regional outages and national and international disruptions.[83] As communications networks move toward a unified next generation network, a single (cyber) attack may become more likely to disrupt all types of communications traffic.

The I&T sector relies to a large extent on security through obscurity. Knowledge about the overall network topology and the exact location of some critical communication nodes is relatively limited and not widely disseminated. Some communications protocols used to manage and control the exchange of information are relatively obscure. This helps minimize the danger of attacks. Obscurity should not be the only defense. An insider with specialized knowledge in the service of a foreign nation or terrorist group could cause a lot of damage.

The complexity of the I&T sector could be a double-edged sword. While it may serve to help protect communications systems against attacks, it also hides potential vulnerabilities and interconnections with other infrastructure sectors that could, one day, lead to massive disruptions or cascading outages.

[83] A large-scale coordinated attack against several or many communication nodes would be extremely difficult to plan and execute – especially without attracting attention from American homeland security and intelligence agencies. Nonetheless, it would not be impossible.

Section II - Routers

Routers are key components of the Internet's infrastructure. These devices direct the flow of traffic around the web, seeking the fastest and most efficient route between two points.[84] As all communications traffic increasingly relies on IP-based data exchanges, the importance of routers will be elevated in the coming years. In the case of the next generation network, routers will be responsible for the safe transportation of all kinds of communications traffic - not just Internet traffic – making them even more vital.

Reports of router vulnerabilities and the potential of cyber attacks against, or using, these systems are on the rise. These devices are crucial to the proper functioning of the Internet, but relatively little analysis of their vulnerabilities and their communication protocols has been done.

Mounting Router Vulnerabilities

Routers are vulnerable in a number of ways. Surprisingly, routers are often not as well secured, configured, or monitored as other online systems. Unauthorized intruders have been able to gain access to, and take control of, routers using default vendor passwords or vendor back doors, or by 'sniffing' for the password.[85] In addition, many large networks and ISPs allow remote access to their routers via the Internet for a variety of reasons. That means that one can telnet or HTTP to a router, potentially allowing an attacker to run malicious code and take over the device.

Furthermore, routers, like other devices, are prone to vulnerabilities. In November 2001, Cisco Systems, the global market leader for routers, announced that its series 12000 routers (commonly used in the Internet's backbone) contained a flaw that made them vulnerable to denial of service (DoS) attacks. By sending fragmented data packets, an attacker could cause the router to generate a large number of Internet Control Message Protocol (ICMP) Unreachable packets, thereby potentially crashing the device.[86] Other vulnerabilities are regularly discovered in the routing infrastructure.[87]

BGP Vulnerabilities

The Border Gateway Protocol (BGP) – the language backbone routers use to communicate with one another – is also a potential avenue for hackers to attack a router

[84] For more information on Internet routing, see Routing in the Internet - http://www.scit.wlv.ac.uk/~jphb/comms/iproute.html

[85] In many cases, default passwords (like 'cisco' for Cisco routers) are never changed by system operators, or vendor back doors are left wide open on active systems 'Trends in Denial of Service Attack Technology', Kevin J. Houle and George M. Weaver, CERT Coordination Center, October 2001 - http://www.cert.org/archive/pdf/DoS_trends.pdf or 'Bugwatch: Routing out hackers', Eric Chien, vnunet.com, September 11, 2001 - http://www.vnunet.com/News/1126754

[86] 'Cisco Routers Vulnerable to DoS', Rene Millman, vnunet.com, November 15, 2001 - http://www.vnunet.com/News/1126889

[87] For an up-to-date list of Cisco Systems security advisories, see Cisco Product Security Incident Response Advisories - http://www.cisco.com/warp/public/707/advisory.html

or compromise it for attacks against other systems.[88] The relative obscurity of the protocol had been its best defense mechanism. As knowledge about BGP spreads, misuse of the protocol could have dangerous consequences. Authentication of BGP messages between routers is currently inadequate. Message authentication - using an MD5 hash - is available to validate the sender of the BGP message, but this is seldom used. This could lead to manipulation, including injecting false routes into a device's routing table or crashing the system. A secure version of BGP, S-BGP, is under development that "uses PKI (Public Key Infrastructure) to authenticate the ownership of an IP address block, Autonomous System numbers and the BGP router's identity."[89] S-BGP would secure the confidentiality and integrity of the BGP messages exchanged between routers. However, implementation of what amounts to a new standard would require the cooperation of Internet registries, router vendors and Internet service providers (ISPs).

SNMP Vulnerabilities Affect Routers

Vulnerabilities discovered in February 2002 in the Simple Network Management Protocol (SNMP) v.1 could also affect network routers. Exploits for these SNMP flaws could target backbone routers, potentially taking over some of these systems or using them as launch pads for DoS attacks.[90]

Possible Router Attacks

Routers are vulnerable in a number of ways. Exploiting these router vulnerabilities could enable a cyber attacker to: take over or disrupt the routers themselves; use compromised routers to inject false routing information into the routing system or to disrupt other routers; or use them as launch pads for scans or attacks against other systems.

A router could be crashed or compromised to take out one of the Internet's communication nodes or manipulate traffic. Simply crashing or overloading one or many routers could result in slowdowns in the flow of data around the Internet.

Router security flaws can be exploited to "modify, delete, or inject routes into the global Internet routing tables to redirect traffic destined for one network to another, effectively causing a denial of service to both (one because no traffic is being routed to them, and the other because they're getting more traffic than they should)."[91] This can be done by, for instance, spoofing Routing Information Protocol (RIP) packets. Many routers use RIP to broadcast and update routing tables. This technique can also have the effect of creating an Internet 'black hole'. Routers are fed incorrect paths that send packets to parts of the

[88] Each router builds a BGP routing table, or route information base (RIM), from the accumulated routes of its neighbors. From all these routing options, the router chooses its 'best route' for each IP block based on established criteria or a local policy. This route alone is then broadcast as the best way to reach the IP block.
[89] 'Latest Hacker Target: Routers', Rutrell Yasin, Internetweek.com, December 17, 2001 - http://www.internetweek.com/story/INW20011217S0004
[90] See ''Devices at risk' from SNMP exploits', James Middleton, vnunet.com, February 15, 2002 - http://www.vnunet.com/News/1129277 or 'Patching the Net's Fatal Flaws', Alex Salkever, Business Week, February 20, 2002 - http://www.businessweek.com/bwdaily/dnflash/feb2002/nf20020220_5030.htm
[91] 'Overview of Attack Trends', Op. Cit.,

Internet where they will be lost. Or, data can be redirected somewhere where it can be viewed or manipulated by an attacker before sending it to its legitimate destination.

Through this technique of injecting false routes – bogus BGP announcements – into the routing tables of core or backbone routers, small changes could have devastating effects. For instance, due to a combination of mistakes and glitches, Internet service providers lost contact with nearly all of the U.S. Internet backbone operators on April 23, 1997 after MAI Network Services in McLean, Virginia, was allowed to provide backbone ISPs with incorrect routing tables. The episode led to much of the Internet being disconnected for up to three hours.[92]

ISPs' filtering policies have, in many cases, been revised to prevent a repetition of this episode. Many ISPs now use 'dense filtering' (prefix-based filtering) at less trusted routing boundaries and 'sparse filtering' (AS-based filtering) at trusted gateways.[93] Many top-level ISPs use static configurations of primary and backup routes in BGP border routers for security reasons and to minimize the likelihood of importing errors from lower tier service providers. 'Policy-based filtering' determines which parts of the Internet's address space neighbors can provide information about by stipulating which routing information "will be accepted from (ingress) or sent to (egress) a particular neighbor."[94] In this fashion, a certain level of security checking is introduced because routers are only allowed to pass on routes they are expected to know via a designated connection – i.e. the link that is known to exist between the two routers (authentication by IP address) – with a password. While this usually prevents the injection of false routes into the system, it also negates the advantage of dynamic re-routing if a path becomes unavailable.[95]

If proper filtering policies are not implemented, "Virtually any router can represent itself as a best path to any destination as a way of intercepting, blocking, or modifying traffic to that destination. Most vulnerable are the interconnection points between major ISPs, where there are no grounds at all for rejecting route advertisements."[96] Even worse, if one router in the exchange has been hacked (compromised through the exploitation of a vulnerability), its trusted relationships with other routers can be exploited to inject false routes or cause other disruptions – this is particularly worrying in the case of backbone routers or critical BGP border routers.

[92] See RISKS-LIST: Risks-Forum Digest, Friday 2 May 1997, Volume 19: Issue 12 - http://www.infowar.com/iwftp/risks/risks-19/19_12.txt or 'Routing Instability on the Internet', Rik Farrow, Network Magazine, March 4, 2002 - http://www.networkmagazine.com/article/NMG20020304S0007
[93] 'A Route-Filtering Model For Improving Global Internet Routing Robustness', iops.org, 1997. Also see 'BGP Route Aggregation and Filtering Policy', Internet Backbone Operations, SprintLink - http://www.sprintlink.net/policy/bgp_filters.html
[94] 'Routing Instability on the Internet', Op. Cit.,
[95] The National Research Council says: "A routing protocol must resolve the tension between (1) performance gains possible given information about the far reaches of the network and (2) increased vulnerability that such dependence can bring. By trusting information received from other domains, a router can calculate near-optimal routes, but such routes are useless if based on inaccurate information provided by malicious or malfunctioning routers." 'Trust in Cyberspace', Op. Cit.,
[96] Ibid.,

Routers as Attack Agents

In addition to becoming targets of cyber attacks, routers are being compromised as potential attack agents. Routers are increasingly being used to conduct reconnaissance, scan for vulnerable systems, obfuscate the origins of cyber strikes, and launch packet flooding DoS attacks.[97] Routers are designed to handle large volumes of traffic. If an attacker is able to compromise a router and redirect the traffic to a single destination, that system will be overwhelmed with data packets, thereby knocking it offline. This effect is magnified if several compromised routers are used in an attack. Reports have emerged that unknown individuals or groups are assembling networks of hundreds of hacked routers. No system on the Internet would be able to defend against an attack launched from one of these networks. Such an attack could easily target other crucial I&T switches or routers.

Consequences of Router Attacks

Routers usually do not authenticate the information they receive, thereby allowing 'bad' data to enter the routing system if a 'trusted' router is taken over or manipulated. Attacks against Internet routers can be used to gain unauthorized access to data packets, manipulate communications, and take out communication nodes or sectors of the web. They may even be able to cripple the Internet temporarily, but no specific open source information is available on this subject.

Security

Basic security improvements are easily achieved by changing default passwords, removing vendor back doors, properly configuring devices, disabling unnecessary services, and implementing sensible routing policies. Other measures, like agreeing upon the introduction of a secure version of BGP that supports encrypted authentication, could be more cumbersome. Schemes to provide routers with global information on the Internet's topology to prevent false route advertisements from entering routing tables have also been proposed, but these currently appear impractical.[98] Simply raising security awareness, increasing system logging and regularly conducting security audits, could pay dividends.[99]

A Look Ahead

Vulnerabilities are regularly discovered in Internet routers. Knowledge about formerly obscure technologies and protocols, such as BGP, is becoming diffused to a wider group of people. Toolkits and attacks scripts for routers are becoming freely available on hacker websites. As router software advances to support loadable kernel modules, this could afford attackers additional opportunities to obtain administrator level access to routers.[100]

---

[97] For more details see 'Trends in Denial of Service Attack Technology', Op. Cit.,
[98] See 'Trust in Cyberspace', Op. Cit.,
[99] In this context, a Router Audit Tool (RAT) for Cisco Systems hardware, developed jointly by the SANS (System Administration, Networking and Security) Institute, UUNet, Cable &Wireless plc, the National Security Agency (NSA) and the Center for Internet Security, was released in February 2002 to rate router security in relation to NSA guidelines. See 'Security Group Pinpoints Cisco Router Weakness', Caron Carlson, eWeek, February 20, 2002 - http://www.eweek.com/article2/0,3959,32301,00.asp
[100] 'Cisco IOS loadable modules pose hacker risk', John Leyden, The Register, December 11, 2001 - http://www.theregister.co.uk/content/55/23316.html

Conclusions

Overall, the routing infrastructure is relatively robust. Although only two manufacturers (Cisco about 60%, Juniper about 35%) dominate the router market, they offer a multitude of products. Any vulnerability in one of these products would only affect a small number of routers overall, especially since many high-value routers are patched as soon as a fix is available. Major backbone and ISP border routers are programmed to filter information so that the possibility of manipulation is decreased. The routing system is designed to be adaptive, dynamic and redundant. If a router is taken offline by an attack, its neighbors will simply start re-routing data to avoid the damaged node.

Yet, some routers are more important than others. As discussed earlier, the bulk of electronic communications travel through a small number of large networks. Attacking routers at the gateways of these networks could have a detrimental effect on the flow of data. Furthermore, a router's ability to respond effectively to an outage or attack may be limited. "To prevent instabilities and oscillations that might occur in the event of transient failures, routing algorithms are designed to not respond immediately to reports of communication link failures. In addition, to provide increased stability, particularly in the face of possible attacks or configuration errors by other network operators, ISPs may rely on static configuration of major routes across network boundaries. These require explicit intervention to respond to some link failures."[101] Moreover, there may not be sufficient capacity elsewhere in the network to carry the traffic diverted due to an outage.

All this does not currently pose an immediate threat to the I&T infrastructure sector as a whole, but does hold the scepter of isolated outages. As attack techniques develop and new vulnerabilities are discovered, a coordinated, large-scale attack on the Internet's routers becomes a more substantive threat with the potential to bring the flow of data to a halt, at least temporarily.

[101] 'The Internet's Coming of Age', Op. Cit.,

Bibliography

Information and Telecommunications Sector

Reports

- 'The National Strategy for Homeland Security', Office of Homeland Security, June 2002 - http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf
- 'The National Strategy to Secure Cyberspace – Draft Version', The President's Critical Infrastructure Protection Board, September 18, 2002 - http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf
- 'Information and Communications Sector Input into the National Strategy for Critical Infrastructure and Cyberspace Security', Prepared by the Cellular Telecommunications and Internet Association (CTIA); Information Technology Association of America (ITAA); Telecommunications Industry Association (TIA); United States Telecom Association (USTA); and Their members in support of the President's Critical Infrastructure Protection (CIP) Program, May 2002 - http://www.pcis.org/getDocument.cfm?urlLibraryDocID=32
- 'Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks', Dr. Adam Cobb, Foreign Affairs, Defence and Trade Group, June 29, 1998 - http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm
- 'In Bits and Pieces – Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society', Ir. H.A.M. Luiijf and Dr. M.H.A. Klaver, Issue Paper for the 'Vulnerabilities in ICT-networks' Infodrome workshop in Amsterdam, March 2000 - http://www.tno.nl/instit/fel/refs/pub2000/luiijf_bitbreuk_english.pdf
- 'Trust in Cyberspace', Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, National Academy Press, Washington D.C., 1999 - http://www.nap.edu/books/0309065585/html/index.html
- 'The Internet's Coming of Age', Computer Science and Telecommunications Board, 2001 - http://bob.nap.edu/html/coming_of_age/
- 'Network Security / Vulnerability Assessments Task Force Report', The President's National Security Telecommunications Advisory Committee, March 2002 - http://www.ncs.gov/nstac/NSVATF-Report-(FINAL).htm
- '"Last Mile" Bandwidth Availability Task Force (LMBATF) Report', The President's National Security Telecommunications Advisory Committee, March 2002 - http://www.ncs.gov/nstac/LMBATF-Report-(FINAL).htm
- 'Convergence Task Force Report - Understanding Convergence and Interconnection of Emerging Networks – NGN Convergence: Security Issues and Recommendations', The President's National Security Telecommunications Advisory Committee, June 2001 - http://www.ncs.gov/nstac/ConvergenceReport-Final.htm
- 'The NSTAC's Response to the National Plan', The President's National Security Telecommunications Advisory Committee, April 2001 - http://www.ncs.gov/nstac/NationalPlanReport-Final.htm
- 'The Future of Our Nation's Communications Infrastructure – A Report to the Nation', Network Reliability and Interoperability Council V, January 4, 2001 - http://www.nric.org/pubs/nric5/reporttothenation.doc
- 'Exploring Solutions for Communications Reliability' – National Communications System, Fiscal Year 2001 - http://www.ncs.gov/pdf/ncs_fy2001_report.pdf
- 'The Cyber-Posture of the National Information Infrastructure', William H. Ware, RAND Corporation, 1998 - http://www.rand.org/publications/MR/MR976/mr976.html#pref
- 'Blue Cascades – Infrastructure Interdependencies Table-Top Exercise - Final Report and Executive Summary,' Pacific Northwest Economic Region, Partnership for Regional Infrastructure Security, July 18, 2002 – http://www.pnwer.org/pris/CascadesReport.htm

- 'An Assessment of the Risk to the Security of Public Networks,' The Network Security Information Exchanges, National Communications System, Washington, D.C., December 12, 1995
- 'Building a 21st Century Telecoms Infrastructure – Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations', Downtown Alliance, Association for a Better NY, NY Building Congress and the Real Estate Board of NY, August 2002
- 'Network Reliability Steering Committee – Annual Report 2001', Network Reliability Steering Committee - http://www.atis.org/pub/nrsc/2001rpt.pdf
- 'Macro-Analysis: First Quarter 2002', Alliance for Telecommunications Industry Solutions', Network Reliability Steering Committee, P.J. Aduskevicz, Chair, NRSC - http://www.atis.org/pub/nrsc/1Q02macanal.pdf
- 'Institute for Telecommunication Sciences 2001 Technical Progress Report', Donald L. Evans, Secretary, Nancy J. Victory, Assistant Secretary for Communications & Information, U.S. Department of Commerce, January 2002 - http://www.its.bldrdoc.gov/tpr/2001/
- 'America's Vulnerability to a Different Nuclear Threat: An Electromagnetic Pulse', Jack Spence, The Heritage Foundation, May 26, 2002 - http://www.heritage.org/Research/MissileDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=12840
- 'Telecommunications Technology – Fact Sheet', Australian Department of Communications, Information Technology and the Arts, December 1999 - http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&ID=997
- 'Overview of Attack Trends', CERT Coordination Center, April 8, 2002 - http://www.cert.org/archive/pdf/attack_trends.pdf
- 'Riptech Internet Security Threat Report – Attack Trends for Q3 and Q4 2001', Riptech Inc., January 2002 - http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report.20020128.pdf
- 'Survey Results – Research on BIND Security', Men & Mice, March 2001 - http://www.menandmice.com/6000/6200_bind_research.html

Public Remarks

- 'Address by John C. Gannon, Assistant Director of Central Intelligence for Analysis and Production to The National Security Telecommunications and Information Systems Security Committee', April 3, 2001 - http://www.fas.org/irp/cia/product/adci_040301.html
- 'Testimony of Joel C. Willemssen, Managing Director, Information Technology Issues, United States General Accounting Office' before the U.S. Senate Committee on Government Affairs, September 12, 2001 - http://www.iwar.org.uk/cip/resources/senate-sep-12-01/091201willemsson.htm
- 'A Supervisory Perspective on Disaster Recovery and Business Continuity', Remarks by Vice Chairman Roger W. Ferguson Jr. before the Institute of International Bankers, Washington D.C., March 4, 2002 - http://www.federalreserve.gov/boarddocs/speeches/2002/20020304/default.htm

Books

- 'Telecom Crash Course', Steven Shepard, McGraw-Hill, 2002
- 'Telecommunications Convergence', Steven Shepard, McGraw-Hill, 2000
- 'The Essential Guide to Telecommunications – 2nd Ed.', Annabel Z. Dodd, Prentice Hall PTR, 2000
- 'Newton's Telecom Dictionary', Harry Newton, CMP Books, 2002

Technical Papers - Tutorials

- 'How the Internet Infrastructure Works', Jeff Tyson, Verizon Learning Center - http://www22.verizon.com/about/community/learningcenter/articles/displayarticle1/0%2C4065%2C1024z1%2C00.html

- 'NAPs, Exchange Points and Interconnections of Internet Service Providers: Recent Trends Part I: 2000 Survey of Worldwide NAPs and Exchange Points', Jeffrey Baker, ep.net, March 31, 2000 - http://www.ep.net/ep-rpt-sum.html
- 'Internet Service Providers and Peering', William B. Norton, - http://www.cs.ucsd.edu/classes/wi01/cse222/papers/norton-isp-draft00.pdf
- 'Strategies for Navigating the Convergence of Voice and Data Networks', May 11, 1998 - http://www.cs.berkeley.edu/~rhuang/290x/final/finalproject.html#circuit
- 'Satellites in Today's Internet – White Paper', Kul Bhasin and Eric A. Bobinsky, Workshop on Research Directions for the Next Generation Internet, Vienna, Va., May 13-14, 1997 - http://www.cra.org/Policy/NGI/papers/bhasinWP
- 'Security for the NGI – White Paper', Steve Bellovin, AT&T Labs, Workshop on Research Directions for the Next Generation Internet, Vienna, Va., May 13-14, 1997 – http://www.cra.org/Policy/NGI/papers/bellovin
- 'Survivability & Trust – White Paper', L. Jean Camp David A. Evensky, Workshop on Research Directions for the Next Generation Internet, Vienna, Va., May 13-14, 1997 – http://www.cra.org/Policy/NGI/papers/campWP
- 'Security in the Traditional Telecommunications Networks and in the Internet', Markus Isomäki, Department of Computer Science, Helsinki University of Technology, November 29, 1999 - http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/tradsec/security_comparison.html
- 'Tutorial on the Design and Construction of Local and Regional Exchange Facilities – Version 0.3', Bill Woodcock, Packet Clearing House, March 2001 - http://www.pch.net/documents/tutorials/ep-construction/ep-construction.html
- 'Tutorial on Free Space Optical Communications', Office of Engineering and Technology, Federal Communications Commission (FCC), September 16, 2002 - http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-02-2291A1.txt
- 'Traffic Engineering for the New Public Network – White Paper', Chuck Semeria, Juniper Networks, September 2000 - http://www.juniper.net/techcenter/techpapers/200004.pdf
- 'Topology discovery by active probing', Bradley Huffaker, Daniel Plummer, David Moore, and k claffy, Cooperative Association for Internet Data Analysis – CAIDA, San Diego Supercomputer Center, University of California, San Diego, 2002 - http://www.caida.org/outreach/papers/2002/SkitterOverview/skitter_overview.pdf
- 'A Step-by-Step Migration Scenario From PSTN to NGN – Technical Paper', Alcatel, January 3, 2002 - http://www6.alcatel.com/homepage/builder.jhtml?content=/publications/abstract.jhtml&repositoryItem=/x/articlepaperlibrary/vndmigration.jhtml
- 'Wiring the World – A Telecommunications Infrastructure Assessment', Steven Shepard, March 29, 2002 - http://www.shepardcomm.com/images/Wiring%20the%20World.pdf
- 'SS7 Tutorial', Performance Technologies - http://www.pt.com/tutorials/ss7/
- 'SS7 Tutorial – Network Architecture', Enhanced Services Division - http://ppchq.org/texts/ss7_architecture.pdf
- ''Real world' trends in perimeter security', NTA Monitor, 2002 - http://www.nta-monitor.com/news/2002-survey.htm
- 'Root Name Server Operational Requirements', Network Working Group, The Internet Society, June 2002 - http://www.ietf.org/rfc/rfc2870.txt?number=2870

Online Resources

- The President's National Security Telecommunications Advisory Committee website - http://www.ncs.gov/nstac/attf.html#One
- 'The Government Emergency Telecommunications Service (GETS) program' - http://gets.ncs.gov/
- 'Our Nation's Critical Infrastructures – Working Definitions', President's Commission on Critical Infrastructure Protection (PCCIP) - http://www.info-sec.com/pccip/web/glossary.html
- 'Telco Building Boom', Telephony, September 11, 2000 - http://www.layerone.com/company/news/000911_Telephony.pdf

- 'Carrier-class Telecom Hotels', Wave Exchange - http://www.carrierhotels.com/properties/waveexchange/pdfs/WaveExchange.pdf
- 'The Internet's Physical Layers', Russ Haynal - http://navigators.com/sessphys.html
- 'Internet: "The Big Picture"', Russ Haynal - http://navigators.com/internet_architecture.html
- Exchange Point Information - http://www.ep.net/
- 'Internet Provider Map' - http://www.amazing.com/internet/internet-map.html
- 'An Atlas of Cyberspaces' - http://www.cybergeography.org/atlas/atlas.html
- 'AT&T Crash Statement: The Official Report', RISKS-LIST: RISKS-FORUM Digest, Forum on Risks to the Public in Computers and Related Systems, Volume 9:Issue 63, January 31, 1990 - http://www.infowar.com/iwftp/risks/Risks-9/risks-9.63.txt
- 'Root Nameserver Year 2000 Status', David Konrad, Akira Kato and Bill Manning, July 15, 1999 - http://www.icann.org/committees/dns-root/y2k-statement.htm
- The Internet Assigned Numbers Authority – Top-Level Domains - http://www.iana.org/domain-names.htm
- Internet Domain Name System Root Servers - http://www.wia.org/pub/rootserv.html
- Domain Name Service - http://www.scit.wlv.ac.uk/~jphb/comms/dns.html

Media Articles

- 'Digital Destruction Was Worst Imaginable', Dan Verton, Computerworld, March 4, 2002 - http://www.computerworld.com/managementtopics/management/recovery/story/0,10801,68762,00.html
- 'Networks at Risk: Assessing Vulnerabilities', Dana Coffield, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,98634,00.asp
- 'Network Edge', Todd Spangler, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,106783,00.asp
- 'Telco Center', Max Smetannikov, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,128463,00.asp
- 'Metro Rings', Bill Scanlon, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,99162,00.asp
- 'Circuit-Switched Networks', Bill Scanlon, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,130672,00.asp
- 'Wireless', Nancy Gohring, eWeek, September 24, 2002 - http://www.eweek.com/article2/0,3959,124583,00.asp
- 'Cable', Richard Williamson, eWeek, September 24, 2001 - http://www.eweek.com/article2/0,3959,130673,00.asp
- 'Phone Network is Vulnerable, Report Finds', Jayson Blair, New York Times, August 6, 2002 - http://www.nytimes.com/2002/08/06/nyregion/06TELE.html?ex=1029297600&en=71b910f1a0c8d94d&ei=5007&partner=USERLAND
- 'Attacks in New York provide sobering lessons', Mike Fish, CNN, January 16, 2002 - http://www.cnn.com/SPECIALS/2002/prepared.cities/stories/new.york.html
- 'Text Messaging to the Rescue', Alex Daniels and Brendan Barrett, Washtech, September 25, 2001
- 'Code Red 'was never a threat'', Mark Ward, BBC News, August 2, 2001 - http://news.bbc.co.uk/2/hi/sci/tech/1470246.stm
- 'Tunnel Burns, Internet Melts', Michaela Cavallaro, The Industry Standard, July 20, 2001 - http://www.thestandard.com/article/0,1902,28110,00.html
- 'Fire's effects ripple onto the Net', Sandeep Junnarkar, C-Net news, July 19, 2001 - http://news.com.com/2100-1033-270217.html
- 'Worldcom Turns Up Two New Internet Public Peering Exchanges', CNN, June 17, 2002
- 'New system keeps phone lines open', Dibya Sarkar, Federal Computer Week, September 18, 2002 - http://www.fcw.com/geb/articles/2002/0916/web-phone-09-18-02.asp
- 'Security requires 'defense in depth', AT&T researcher says', Loring Wirbel, CommsDesign.com, September 10, 2002 - http://www.commsdesign.com/story/OEG20020910S0011

- 'Telecom Industry Beefs Up Priority Wireless Access, Backbone Security', Dan Verton, Computerworld, September 9, 2002 - http://www.computerworld.com/securitytopics/security/story/0,10801,74076,00.html
- 'The ISP Top Dogs', Denise Pappalardo, Network World Fusion, May 30, 2001 - http://www.nwfusion.com/newsletters/isp/2001/00846039.html
- 'Cyberterrorism Scenario Scrutinized', Gretel Johnston, PC World, August 21, 2002 - http://www.pcworld.com/news/article/0,aid,104271,00.asp
- 'Computer Problems Snarl MARC's Evening Rush', Lyndsey Layton, Washington Post, August 6, 2002
- 'ICANN Panel Weighs DNS Vulnerabilities', Patrick Thibodeau, Computerworld, February 25, 2002 - http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,68588,00.html
- 'Bind vulnerability threatens web hosts', vnunet.com, July 2, 2001 - http://www.vnunet.com/News/1120756
- 'ICANN: To Serve and Protect', Declan McCullagh, Wired News, November 13, 2001 - http://www.wired.com/news/politics/0,1283,48344,00.html
- 'Icann warns of worldwide net threat', James Middleton, vnunet.com, November 14, 2001 - http://www.vnunet.com/News/1126863
- 'Internet outages until 2006 says Gartner', Nick Farrell, vnunet.com, November 20, 2001 - http://www.itweek.co.uk/News/1126993
- 'Study: Many companies still vulnerable to DNS outage', Stacy Cowley, Infoworld, October 4, 2001 - http://www.infoworld.com/articles/hn/xml/01/10/04/011004hnmice.xml
- 'The Internet root's alright, says Icann', James Middleton, vnunet.com, November 22, 2001 - http://www.vnunet.com/News/1127075

Routers

Reports – Technical Papers

- 'Internet Monitoring and Historical Route Archive using the Border Gateway Protocol: Progress Report August 2002', Dennis McGrath and George Cybenko, Institute for Security Technology Studies, August 2002
- 'Trends in Denial of Service Attack Technology', Kevin J. Houle and George M. Weaver, CERT Coordination Center, October 2001 - http://www.cert.org/archive/pdf/DoS_trends.pdf
- 'Improving Security on Cisco Routers', Cisco Systems - http://www.cisco.com/warp/public/707/21.html
- 'BGP Route Aggregation and Filtering Policy', Internet Backbone Operations, SprintLink - http://www.sprintlink.net/policy/bgp_filters.html
- 'A Route-Filtering Model For Improving Global Internet Routing Robustness', iops.org, 1997 - http://www.iops.org/Documents/routing.html

Media Articles

- 'Cisco Routers Vulnerable to DoS', Rene Millman, vnunet.com, November 15, 2001 - http://www.vnunet.com/News/1126889
- 'Latest Hacker Target: Routers', Rutrell Yasin, Internetweek.com, December 17, 2001 - http://www.internetweek.com/story/INW20011217S0004
- 'Hackers Attacking Routers in Greater Numbers', George V. Hulme, Information Week, October 31, 2001 - http://www.informationweek.com/story/IWK20011031S0006
- ''Devices at risk' from SNMP exploits', James Middleton, vnunet.com, February 15, 2002 - http://www.vnunet.com/News/1129277
- 'Patching the Net's Fatal Flaws', Alex Salkever, Business Week, February 20, 2002 - http://www.businessweek.com/bwdaily/dnflash/feb2002/nf20020220_5030.htm
- 'Cisco IOS loadable modules pose hacker risk', John Leyden, The Register, December 11, 2001 - http://www.theregister.co.uk/content/55/23316.html

- 'Security Group Pinpoints Cisco Router Weakness', Caron Carlson, eWeek, February 20, 2002 - http://www.eweek.com/article2/0,3959,32301,00.asp
- 'Cisco routers vulnerable to easy attack', Thomas C. Greene, The Register, June 28, 2000 - http://www.theregister.co.uk/content/archive/11626.html
- 'Strategies & Issues: Ports of Entry -- Routers in the Crosshairs', Curtis E. Dalton April 5, 2002 - http://www.networkmagazine.com/article/NMG20020401S0002/2
- 'Routing Instability on the Internet', Rik Farrow, Network Magazine, March 4, 2002 - http://www.networkmagazine.com/article/NMG20020304S0007
- 'Bugwatch: Routing out hackers', Eric Chien, vnunet.com, September 11, 2001 - http://www.vnunet.com/News/1126754

Online Resources

- RISKS-LIST: Risks-Forum Digest, May 2, 1997, Volume 19:Issue 12 - http://www.infowar.com/iwftp/risks/risks-19/19_12.txt
- Cisco Product Security Incident Response Advisories - http://www.cisco.com/warp/public/707/advisory.html
- Routing in the Internet - http://www.scit.wlv.ac.uk/~jphb/comms/iproute.html